kaspersky

Kaspersky Embedded Systems Security 3.4 for Windows

© 2024 AO Kaspersky Lab

Contents

About Kaspersky Embedded Systems Security for Windows

What's new

Sources of information about Kaspersky Embedded Systems Security for Windows

- Sources for independent retrieval of information
- Discussing Kaspersky applications on the Forum

Kaspersky Embedded Systems Security for Windows

- Distribution kit
- Software and hardware requirements
- Functional requirements and limitations
  - Installation and uninstallation
  - File Integrity Monitor
  - Firewall Management
  - Other limitations

Installing and removing the application

- About Kaspersky Embedded Systems Security for Windows update
- Migrating settings values of the updated application version
- About Kaspersky Embedded Systems Security for Windows Administration Tools update
- Kaspersky Embedded Systems Security for Windows software component codes for the Windows Installer service
  - Kaspersky Embedded Systems Security for Windows software components
  - "Administration tools" software component
- System changes after Kaspersky Embedded Systems Security for Windows installation
- Kaspersky Embedded Systems Security for Windows processes
- Installation and recovery settings, and Windows Installer command-line options
- Kaspersky Embedded Systems Security for Windows install and uninstall logs
- Installation planning
  - Selecting administration tools
  - Selecting the installation type
- Installing and uninstalling the application using a wizard
  - Installing using the Setup Wizard
    - Kaspersky Embedded Systems Security for Windows installation
    - Kaspersky Embedded Systems Security for Windows Console installation
    - Advanced settings after installation of the Application Console on another device
      - Allowing anonymous remote access to COM applications
      - Allowing network connections for the Kaspersky Embedded Systems Security for Windows remote management process
      - Adding outbound rule for Windows Firewall
    - Actions to perform after Kaspersky Embedded Systems Security for Windows installation
      - Starting and configuring Kaspersky Embedded Systems Security for Windows Database Update task
      - Critical Areas Scan
  - Modifying the set of components and repairing Kaspersky Embedded Systems Security for Windows
  - Uninstalling using the Setup Wizard
    - Kaspersky Embedded Systems Security for Windows uninstallation
    - Kaspersky Embedded Systems Security for Windows Console uninstallation
- Installing and uninstalling the application from the command line
  - About installing and uninstalling Kaspersky Embedded Systems Security for Windows from command line
  - Example commands for installing Kaspersky Embedded Systems Security for Windows

Actions to perform after Kaspersky Embedded Systems Security for Windows installation
Adding / removing components. Sample commands
Kaspersky Embedded Systems Security for Windows uninstallation. Sample commands
Return codes
Installing and uninstalling the application using Kaspersky Security Center
General information about installing via Kaspersky Security Center
Rights to install or uninstall Kaspersky Embedded Systems Security for Windows
Installing Kaspersky Embedded Systems Security for Windows via Kaspersky Security Center
Actions to perform after Kaspersky Embedded Systems Security for Windows installation
Installing the Application Console via Kaspersky Security Center
Uninstalling Kaspersky Embedded Systems Security for Windows via Kaspersky Security Center
Installing and uninstalling via Active Directory group policies
Installing Kaspersky Embedded Systems Security for Windows via Active Directory group policies
Actions to perform after Kaspersky Embedded Systems Security for Windows installation
Uninstalling Kaspersky Embedded Systems Security for Windows via Active Directory group policies
Checking Kaspersky Embedded Systems Security for Windows functions. Using the EICAR test virus
About the EICAR test virus
Checking the Real-Time File Protection and On-Demand Scan features
Application interface
Application licensing
About the End User License Agreement
About the license
About license certificate
About the key
About the key file
About activation code
About data provision
Activating the application with a key file
Activating the application with an activation code
Viewing information about current license
Functional limitations when the license expires
Renewing license
Deleting the key
Working with the Administration Plug-in
Managing Kaspersky Embedded Systems Security for Windows from Kaspersky Security Center
Managing application settings
Navigation
Opening general settings via the policy
Opening general settings in the application properties window
Configuring general application settings in Kaspersky Security Center
Configuring scalability, interface, and scan settings in Kaspersky Security Center
Configuring security settings in Kaspersky Security Center
Configuring connection settings using Kaspersky Security Center
Configuring scheduled start of local system tasks
Configuring Quarantine and Backup settings in Kaspersky Security Center
Creating and configuring policies
Creating a policy
Kaspersky Embedded Systems Security for Windows policy settings sections

Configuring a policy
Creating and configuring tasks using Kaspersky Security Center
About task creation in Kaspersky Security Center
Creating a task using Kaspersky Security Center
Going to the local task settings and general application settings for an individual computer
Configuring group tasks in Kaspersky Security Center
Activation of the Application task
Update tasks
Application Integrity Control
Configuring crash diagnostics settings in Kaspersky Security Center
Managing task schedules
Scheduling tasks
Enabling and disabling scheduled tasks
Reports in Kaspersky Security Center
Working with the Kaspersky Embedded Systems Security for Windows Console
About the Kaspersky Embedded Systems Security for Windows Console
Kaspersky Embedded Systems Security for Windows Console interface
Kaspersky Embedded Systems Security for Windows Console window
System Tray Icon in the notification area
Managing Kaspersky Embedded Systems Security for Windows via the Application Console on another device
Configuring general application settings via the Application Console
Managing Kaspersky Embedded Systems Security for Windows tasks
Kaspersky Embedded Systems Security for Windows task categories
Starting, pausing, resuming, and stopping tasks manually
Managing task schedules
Configuring the task schedule settings
Enabling and disabling scheduled tasks
Using user accounts to start tasks
About using accounts to start tasks
Specifying a user account to start a task
Importing and exporting settings
About importing and exporting settings
Exporting settings
Importing settings
Using security settings templates
About security settings templates
Creating a security settings template
Viewing security settings in a template
Applying a security settings template
Deleting a security settings template
Viewing protection status and Kaspersky Embedded Systems Security for Windows information
Working with the Web Plug-in from Web Console and Cloud Console
Managing Kaspersky Embedded Systems Security for Windows from Web Console and Cloud Console
Web Plug-in limitations
Managing application settings
Configuring general application settings in Web Plug-in
Configuring scalability, interface, and scan settings in Web Plug-in
Configuring security settings in Web Plug-in

Configuring connection settings in Web Plug-in
Configuring scheduled start of local system tasks
Configuring Quarantine and Backup settings in Web Plug-in
Creating and configuring policies
Creating a policy
Kaspersky Embedded Systems Security for Windows policy settings sections
Creating and configuring tasks using Kaspersky Security Center
About task creation in Web Plug-in
Creating a task in Web Plug-in
Configuring group tasks in Web Plug-in
Configuring Activation of the Application task in Web Plug-in
Configuring Update tasks in Web Plug-in
Configuring crash diagnostics settings in Web Plug-in
Managing task schedules
Scheduling tasks
Enabling and disabling scheduled tasks
Reports in Kaspersky Security Center
Compact Diagnostic Interface
About the Compact Diagnostic Interface
Reviewing the Kaspersky Embedded Systems Security for Windows status via the Compact Diagnostic Interface
Reviewing security event statistics
Reviewing current application activity
Configuring writing of dump and trace files
Kaspersky Embedded Systems Security for Windows database and software modules update
About Update tasks
About Software Modules Update
About Database Update
Kaspersky Embedded Systems Security for Windows database and software modules updating schemes
Configuring Update tasks
Configuring settings for working with Kaspersky Embedded Systems Security for Windows update sources
Optimizing disk I/O when running the Database Update task
Configuring Copying Updates task settings
Configuring Software Modules Update task settings
Rolling back Kaspersky Embedded Systems Security for Windows database updates
Rolling back application module updates
Update task statistics
Isolating objects and copying backups
Isolating probably infected objects. Quarantine
About quarantining probably infected objects
Viewing quarantine objects
Sorting quarantined objects
Filtering quarantined objects
Quarantine Scan
Restoring quarantined objects
Moving objects to Quarantine
Deleting objects from Quarantine
Sending probably infected objects to Kaspersky for analysis
Configuring Quarantine settings

Quarantine statistics
Making backup copies of objects. Backup
About backing up objects before disinfection or deletion
Viewing objects stored in Backup
Sorting files in Backup
Filtering files in Backup
Restoring files from Backup
Deleting files from Backup
Configuring Backup settings
Backup statistics
Blocking access to network resources. Blocked network sessions
List of blocked network sessions
Managing the List of blocked network sessions via the Administration Plug-in
Enabling untrusted hosts blocking
Configuring settings for the List of blocked network sessions
Managing the List of blocked network sessions via the Application Console
Enabling untrusted hosts blocking
Configuring settings for the List of blocked network sessions
Managing the List of blocked network sessions via the Web Plug-in
Enabling network sessions blocking
Configuring settings for the List of blocked network sessions
Event registration. Kaspersky Embedded Systems Security for Windows logs
Ways to register Kaspersky Embedded Systems Security for Windows events
System audit log
Sorting events in the system audit log
Filtering events in the system audit log
Deleting events from the system audit log
Task logs
About task logs
Viewing the list of events in task logs
Sorting task logs
Filtering task logs
Viewing statistics and information about a Kaspersky Embedded Systems Security for Windows task in task logs
Exporting information from a task log
Deleting task logs
Security log
Viewing the event log of Kaspersky Embedded Systems Security for Windows in Event Viewer
Configuring log settings via the Application Console
About SIEM integration
Configuring SIEM integration settings
Configuring logs and notifications settings via the Administration Plug-in
Configuring task logs settings
Security log
Configuring SIEM integration settings
Configuring notification settings
Configuring interaction with the Administration Server
Notification settings
Administrator and user notification methods

Configuring administrator and user notifications
Starting and stopping Kaspersky Embedded Systems Security for Windows
Starting the Kaspersky Embedded Systems Security for Windows Administration Plug-in
Starting the Kaspersky Embedded Systems Security for Windows Console from the Start menu
Starting and stopping the Kaspersky Security Service
Starting Kaspersky Embedded Systems Security for Windows components in the operating system safe mode
About Kaspersky Embedded Systems Security for Windows working in the operating system safe mode
Starting Kaspersky Embedded Systems Security for Windows in safe mode
Kaspersky Embedded Systems Security for Windows self-defense
About Kaspersky Embedded Systems Security for Windows self-defense
Protection from changes to folders with installed Kaspersky Embedded Systems Security for Windows components
Protection from changes to Kaspersky Embedded Systems Security for Windows registry keys
Registering Kaspersky Security as a protected service
Managing access permissions for Kaspersky Embedded Systems Security for Windows functions
About permissions to manage Kaspersky Embedded Systems Security for Windows
About permissions to manage registered services
About access permissions for the Kaspersky Security Management Service
About permissions to manage the Kaspersky Security Service
Managing access permissions via the Administration Plug-in
Configuring access permissions for Kaspersky Embedded Systems Security for Windows and the Kaspersky Security Service
Password-protected access to Kaspersky Embedded Systems Security for Windows functions
Managing access permissions via the Application Console
Configuring access permissions for managing Kaspersky Embedded Systems Security for Windows and the Kaspersky Security Service
Password-protected access to Kaspersky Embedded Systems Security for Windows functions
Managing access permissions via the Web Plug-in
Configuring access permissions for Kaspersky Embedded Systems Security for Windows and the Kaspersky Security Service
Password-protected access to Kaspersky Embedded Systems Security for Windows functions
Real-Time File Protection
About the Real-Time File Protection task
About the task protection scope and security settings
About virtual protection scopes
Predefined protection scopes
About predefined security levels
File extensions scanned by default in the Real-Time File Protection task
Default Real-Time File Protection task settings
Managing the Real-Time File Protection task via the Administration Plug-in
Navigation
Opening policy settings for the Real-Time File Protection task
Opening the Real-Time File Protection task settings
Configuring Real-Time File Protection task
Selecting the protection mode
Configuring Heuristic Analyzer and integration with other application components
Scheduling tasks
Creating and configuring the task protection scope
Selecting predefined security levels for On-Demand Scan tasks
Configuring security settings manually

Configuring general task settings
Configuring actions
Configuring performance
Managing the Real-Time File Protection task via the Application Console
Navigation
Opening the Real-Time File Protection task settings
Opening the Real-Time File Protection task scope settings
Configuring Real-Time File Protection task
Selecting protection mode
Configuring Heuristic Analyzer and integration with other application components
Configuring the task schedule settings
Creating the protection scope
Configuring the view for network file resources
Creating the protection scope
Including network objects in the protection scope
Creating a virtual protection scope
Configuring security settings manually
Selecting predefined security levels for Real-Time File Protection task
Configuring general task settings
Configuring actions
Configuring performance
Real-Time File Protection task statistics
Managing Real-Time File Protection task via the Web Plug-in
Configuring Real-Time File Protection task
Configuring the task protection scope
KSN Usage
About the KSN Usage task
Default KSN Usage task settings
Managing KSN Usage via the Administration Plug-In
Configuring KSN Usage task
Configuring Data Processing
Managing KSN Usage via the Application Console
Configuring KSN Usage task
Configuring Data Processing
Managing KSN Usage via the Web Plug-in
Configuring additional data transfer
KSN Usage task statistics
Network Threat Protection
About the Network Threat Protection task
Default Network Threat Protection task settings
Configuring the Network Threat Protection task via the Application Console
General task settings
Adding exclusions
Configuring the Network Threat Protection task via the Administration Plug-in
General task settings
Adding exclusions
Configuring the Network Threat Protection task via the Web Plug-in
General task settings

Adding exclusions
Applications Launch Control
About the Applications Launch Control task
About Applications Launch Control rules
About Software Distribution Control
About KSN usage for the Applications Launch Control task
About the Rule Generator for Applications Launch Control
Default Applications Launch Control task settings
Managing Applications Launch Control via the Administration Plug-in
Navigation
Opening policy settings for the Applications Launch Control task
Opening the Applications Launch Control rules list
Opening the Rule Generator for Applications Launch Control task wizard and properties
Configuring Applications Launch Control task settings
Configuring Software Distribution Control
Configuring a Rule Generator for Applications Launch Control task
Configuring Applications Launch Control rules via the Kaspersky Security Center
Adding an Applications Launch Control rule
Enabling the Default Allow mode
Creating allowing rules for applications launch control from Kaspersky Security Center events
Importing rules from a Kaspersky Security Center report on blocked applications
Importing Applications Launch Control rules from an XML file
Checking application launches
Creating a Rule Generator for Applications Launch Control task
Restricting the task usage scope
Actions to perform during automatic rule generation
Actions to perform upon completion of automatic rule generation
Managing Applications Launch Control via the Application Console
Navigation
Opening the Applications Launch Control task settings
Opening the Applications Launch Control rules window
Opening the Rule Generator for Applications Launch Control task settings
Configuring Applications Launch Control task settings
Selecting the mode of the Applications Launch Control task
Configuring the scope of the Applications Launch Control task
Configuring KSN usage
Configuring Software Distribution Control
Configuring Applications Launch Control rules
Adding an Applications Launch Control rule
Enabling the Default Allow mode
Creating allowing rules from Applications Launch Control task events
Exporting Applications Launch Control rules
Importing Applications Launch Control rules from an XML file
Removing Applications Launch Control rules
Configuring a Rule Generator for Applications Launch Control task
Restricting the task usage scope
Actions to perform during automatic rule generation
Actions to perform upon completion of automatic rule generation

Managing Applications Launch Control via the Web Plug-in
Device Control
About Device Control task
About Device Control rules
Default Device Control task settings
Managing Device Control via the Administration Plug-in
Configuring Device Control task settings
Using Device Control rules
Adding Device Control rules
Viewing Device Control rule properties
Activating and deactivating Device Control rules
Expanding Device Control rules usage scope
Configuring access permissions
Exporting Device Control rules
Creating rules with the Rule Generator for Device Control local task
Generating a Kaspersky Security Center blocked devices report
Managing Device Control via the Application Console
Configuring Device Control task settings
Using Device Control rules
Adding Device Control rules
Exporting Device Control rules
Activating and deactivating Device Control rules
Expanding Device Control rules usage scope
Configuring access permissions
Creating rules using the Rule Generator for Device Control task
Creating a rules XML file from Device Control task events
Managing Device Control via the Web Plug-in
Configuring Device Control task settings
Adding Device Control rules
Configuring access permissions
Exporting Device Control rules
Creating rules with the Rule Generator for Device Control local task
Generating a Kaspersky Security Center blocked devices report
Firewall Management
About the Firewall Management task
About Firewall rules
Default Firewall Management task settings
Configuring the Firewall Management task using the Administration Plug-in
Configuring general settings of the Firewall Management task
Creating and configuring firewall rules
Enabling and disabling Firewall rules
Deleting Firewall rules
Configuring the Firewall Management task using the Application Console
Configuring general settings of the Firewall Management task
Creating and configuring firewall rules
Enabling and disabling Firewall rules
Deleting Firewall rules
Configuring the Firewall Management task using the Web Plug-in

Configuring general settings of the Firewall Management task
Creating and configuring firewall rules
Enabling and disabling Firewall rules
Deleting Firewall rules
File Integrity Monitor
About the File Integrity Monitor task
About file operations monitoring rules
Default File Integrity Monitor task settings
Manage File Integrity Monitor via the Administration Plug-in
Configuring the File Integrity Monitor task
Creating and configuring a file operations monitoring rule
Export and import of file operations monitoring rules
Manage File Integrity Monitor via the Application Console
Configuring the File Integrity Monitor task
Creating and configuring a file operations monitoring rule
Export and import of file operations monitoring rules
Manage File Integrity Monitor via the Web Plug-in
Configuring the File Integrity Monitor task
Creating and configuring a file operations monitoring rule
Export and import of file operations monitoring rules
AMSI Scanner
About the AMSI Scanner task
Default AMSI Scanner task settings
Configuring AMSI Scanner task settings via the Administration Plug-in
Configuring AMSI Scanner task settings via the Application Console
Configuring AMSI Scanner task settings via the Web Plug-in
AMSI Scanner task statistics
Registry Access Monitor
About the Registry Access Monitor task
About the registry access monitoring rules
Default Registry Access Monitor task settings
Managing the Registry Access Monitor via the Administration Plug-in
Configuring the Registry Access Monitor task settings
Creating and configuring a registry access monitoring rule
Export and import of registry access monitoring rules
Managing the Registry Access Monitor task via the Application Console
Configuring general settings of the Registry Access Monitor task
Creating and configuring a registry access monitoring rule
Export and import of registry access monitoring rules
Managing the Registry Access Monitor via the Web Plug-in
Configuring the Registry Access Monitor task settings
Creating and configuring a registry access monitoring rule
Export and import of registry access monitoring rules
Log Inspection
About the Log Inspection task
Default Log Inspection task settings
Managing Log Inspection rules via the Administration Plug-in
Configuring predefined task rules

Adding Log Inspection rules via the Administration Plug-in
Managing Log Inspection rules via the Application Console
Configuring predefined task rules
Adding Log Inspection rules via the Application Console
Managing Log Inspection rules via the Web Plug-in
On-Demand Scan
About On-Demand Scan tasks
About the task scan scope and security settings
Predefined scan scopes
Online storage file scanning
About predefined security levels
Removable Drives Scan
About the Baseline File Integrity Monitor task
Enabling start of On-Demand Scan task from context menu
Default On-Demand Scan tasks settings
Managing On-Demand Scan tasks via the Administration Plug-in
Navigation
Opening the On-Demand Scan task wizard
Opening the On-Demand Scan task properties
Creating an On-Demand Scan task
Assigning the Critical Areas Scan status to an On-Demand Scan task
Running an On-Demand Scan task in the background
Registering execution of a Critical Areas Scan
Configuring the task scan scope
Selecting predefined security levels for On-Demand Scan tasks
Configuring security settings manually
Configuring general task settings
Configuring actions
Configuring performance
Configuring Removable Drives Scan
Configuring a Baseline File Integrity Monitor task
Managing On-Demand Scan tasks via the Application Console
Navigation
Opening the On-Demand Scan task settings
Opening the On-Demand Scan task scope settings
Creating and configuring an On-Demand Scan task
Scan scope in On-Demand Scan tasks
Configuring the view for network file resources
Creating a scan scope
Including network objects in the scan scope
Creating a virtual scan scope
Configuring security settings
Selecting predefined security levels for On-Demand Scan tasks
Configuring general task settings
Configuring actions
Configuring performance
Configuring hierarchical storage
Removable Drives Scan

- On-Demand Scan task statistics
- Creating and configuring a Baseline File Integrity Monitor task
- Managing On-Demand Scan tasks via the Web Plug-in
- Opening the On-Demand Scan task wizard
- Opening the On-Demand Scan task properties
- Configuring the task scan scope
- Configuring the task settings

Trusted zone

- About the Trusted Zone
- Configuring Trusted Zone settings via the Administration Plug-in
- Adding exclusions
- Adding trusted processes
- Configuring certificate monitoring
- Adding certificate monitoring rules
- Exporting certificate monitoring rules
- Applying the not-a-virus mask
- Configuring the Trusted Zone via the Application Console
- Adding an exclusion to the Trusted Zone
- Adding trusted processes
- Configuring certificate monitoring
- Adding certificate monitoring rules
- Exporting certificate monitoring rules
- Applying the not-a-virus mask
- Configuring the Trusted Zone via the Web Plug-in
- Adding exclusions
- Adding trusted processes
- Configuring certificate monitoring
- Adding certificate monitoring rules
- Exporting certificate monitoring rules
- Applying the not-a-virus mask

Exploit Prevention

- About Exploit Prevention
- Managing Exploit Prevention via the Administration Plug-in
- Navigation
- Opening policy settings for Exploit Prevention
- Opening the Exploit Prevention properties window
- Configuring process memory protection settings
- Adding a process to the protection scope
- Managing Exploit Prevention via the Application Console
- Navigation
- Opening the Exploit Prevention general settings
- Opening the Exploit Prevention process protection settings
- Configuring process memory protection settings
- Adding a process to the protection scope
- Managing Exploit Prevention via the Web Plug-in
- Configuring process memory protection settings
- Adding a process to the protection scope
- Exploit prevention techniques

Integrating with third-party systems
Performance counters for System Monitor
About Kaspersky Embedded Systems Security for Windows performance counters
Total number of requests denied
Total number of requests skipped
Number of requests not processed because of lack of system resources
Number of requests sent to be processed
Average number of file interception dispatcher streams
Maximum number of file interception dispatcher streams
Number of elements in the infected objects queue
Number of objects processed per second
Kaspersky Embedded Systems Security for Windows SNMP counters and traps
About Kaspersky Embedded Systems Security for Windows SNMP counters and traps
Kaspersky Embedded Systems Security for Windows SNMP counters
Performance counters
Quarantine counters
Backup counter
General counters
Update counter
Real-Time File Protection counters
Kaspersky Embedded Systems Security for Windows SNMP traps and their options
Kaspersky Embedded Systems Security for Windows SNMP traps options descriptions and possible values
Integrating with WMI
Working with Kaspersky Embedded Systems Security for Windows from the command line
Commands
Displaying command help for Kaspersky Embedded Systems Security for Windows. KAVSHELL HELP
Starting and stopping the Kaspersky Security Service: KAVSHELL START, KAVSHELL STOP
Scanning a specified scope: KAVSHELL SCAN
Starting the Critical Areas Scan task: KAVSHELL SCANCRITICAL
Managing tasks asynchronously: KAVSHELL TASK
Removing the PPL attribute: KAVSHELL CONFIG
Starting and stopping Real-Time Computer Protection tasks. KAVSHELL RTP
Managing the Applications Launch Control task: KAVSHELL APPCONTROL /CONFIG
Rule Generator for Applications Launch Control: KAVSHELL APPCONTROL /GENERATE
Filling the list of Applications Launch Control rules. KAVSHELL APPCONTROL
Filling the list of Device Control rules. KAVSHELL DEVCONTROL
Starting the Database Update task: KAVSHELL UPDATE
Rolling back Kaspersky Embedded Systems Security for Windows database updates: KAVSHELL ROLLBACK
Managing Log Inspection: KAVSHELL TASK LOG-INSPECTOR
Activation of Application. KAVSHELL LICENSE
Enabling, configuring, and disabling trace logs. KAVSHELL TRACE
Kaspersky Embedded Systems Security for Windows log files defragmentation. KAVSHELL VACUUM
Cleaning iSwift base. KAVSHELL FBRESET
Enabling and disabling dump file creation. KAVSHELL DUMP
Importing settings. KAVSHELL IMPORT
Exporting settings. KAVSHELL EXPORT
Integration with Microsoft Operations Management Suite. KAVSHELL OMSINFO
Managing the Baseline File Integrity Monitor task: KAVSHELL FIM /BASELINE

- Command return codes
  - Return code for the KAVSHELL START and KAVSHELL STOP commands
  - Return code for KAVSHELL SCAN and KAVSHELL SCANCRITICAL commands
  - Return code for the KAVSHELL TASK LOG-INSPECTOR command
  - Return codes for the KAVSHELL TASK command
  - Return codes for the KAVSHELL RTP command
  - Return codes for the KAVSHELL UPDATE command
  - Return codes for the KAVSHELL ROLLBACK command
  - Return codes for the KAVSHELL LICENSE command
  - Return codes for the KAVSHELL TRACE command
  - Return codes for the KAVSHELL FBRESET command
  - Return codes for the KAVSHELL DUMP command
  - Return codes for the KAVSHELL IMPORT command
  - Return codes for the KAVSHELL EXPORT command
  - Return codes for the KAVSHELL FIM /BASELINE command
- Contacting Technical Support
  - How to get technical support
  - Technical Support via Kaspersky CompanyAccount
  - Using trace files and AVZ scripts
- Glossary
  - Active key
  - Administration Server
  - Anti-virus databases
  - Archive
  - Backup
  - Disinfection
  - Event importance
  - False positive
  - File mask
  - Heuristic analyzer
  - Infectable file
  - Infected object
  - Kaspersky Security Network (KSN)
  - License term
  - Local task
  - OLE object
  - Policy
  - Protection state
  - Quarantine
  - Security level
  - SIEM
  - Startup objects
  - Task
  - Task settings
  - Update
  - Vulnerability
- Information about third-party code
- Trademark notices

About Kaspersky Embedded Systems Security for Windows

Kaspersky Embedded Systems Security for Windows protects computers and other embedded systems under Microsoft® Windows® (hereinafter also referred to as protected devices) against viruses and other computer threats. Kaspersky Embedded Systems Security for Windows users are corporate network administrators and specialists responsible for anti-virus protection of the corporate network.

The application is not intended to be used in technological processes that involve automated control systems. To protect devices in such systems, it is recommended to use Kaspersky Industrial CyberSecurity for Nodes application.

You can install Kaspersky Embedded Systems Security for Windows on a variety embedded systems under Windows, including the following devices types:

- ATM (automated tellers machines).
- POS (points of sales).

Kaspersky Embedded Systems Security for Windows can be managed in the following ways:

- Via the Application Console installed on the same protected device as Kaspersky Embedded Systems Security for Windows, or on a different device
- Using commands in the command line
- Via the Kaspersky Security Center Administration Console

The Kaspersky Security Center application can also be used for centralized administration of multiple protected devices running Kaspersky Embedded Systems Security for Windows.

It is possible to review Kaspersky Embedded Systems Security for Windows performance counters for the "System Monitor" application, as well as SNMP counters and traps.

Kaspersky Embedded Systems Security for Windows components and functions

The application includes the following components:

- **Real-Time File Protection**. Kaspersky Embedded Systems Security for Windows scans objects when they are accessed. Kaspersky Embedded Systems Security for Windows scans the following objects:
  - Files.
  - Alternate file system streams (NTFS streams)
  - Master boot records and boot sectors on local hard and removable drives
- **On-Demand Scan**. Kaspersky Embedded Systems Security for Windows runs a single scan of the specified area for viruses and other computer security threats. The application scans files, RAM, and autorun objects on a protected device.
- **Applications Launch Control**. The component monitors user attempts to start applications and regulates application launches on the protected device.

- **Device Control**. The component controls registration and usage of external devices in order to protect the device against computer security threats that may arise while exchanging files with USB-connected flash drives or other types of external device.

- **Firewall Management**. This component provides the ability to manage the Windows Firewall: configure settings and operating system firewall rules and block any possibility of external firewall configuration.

- **File Integrity Monitor**. Kaspersky Embedded Systems Security for Windows detects changes in files within the monitoring scopes specified in the task settings. These changes may indicate a security breach on the protected device.

- **Log Inspection**. This component monitors the integrity of the protected environment based on the results of an inspection of Windows event logs.

The following functions are implemented in the application:

- **Database Update** and **Software Modules Update**. Kaspersky Embedded Systems Security for Windows downloads updates of application databases and modules from Kaspersky's FTP or HTTP update servers, Kaspersky Security Center Administration Server, or other update sources.

- **Quarantine**. Kaspersky Embedded Systems Security for Windows quarantines probably infected objects by moving such objects from their original location to the *Quarantine* folder. For security purposes, objects in the Quarantine folder are stored in encrypted form.

- **Backup**. Kaspersky Embedded Systems Security for Windows stores encrypted copies of objects classified as *Infected* in *Backup* before disinfecting or deleting them.

- **Administrator and user notifications**. You can configure the application to notify the administrator and users who access the protected device about the events related to the operation of Kaspersky Embedded Systems Security and the anti-virus protection status of the device.

- **Importing and exporting settings**. You can export Kaspersky Embedded Systems Security for Windows settings to an XML configuration file and import settings into Kaspersky Embedded Systems Security for Windows from the configuration file. You can save all application settings or only settings for individual components to a configuration file.

- **Applying templates**. You can manually configure the security settings of a node in the tree or in a list of the protected device's file resources, and save the configured setting values as a template. This template can then be used to specify the security settings of other nodes in Kaspersky Embedded Systems Security for Windows protection and scan tasks.

- **Managing access permissions for Kaspersky Embedded Systems Security for Windows functions**. You can configure the rights to manage Kaspersky Embedded Systems Security for Windows and the Windows services registered by the application, for users and groups of users.

- **Writing events to the Windows Event Log**. Kaspersky Embedded Systems Security for Windows logs information about software component settings, the current status of tasks, events that occur while tasks run, events associated with Kaspersky Embedded Systems Security for Windows management, and information required to diagnose errors in Kaspersky Embedded Systems Security for Windows.

- **Trusted Zone**. You can generate a list of exclusions from the protection or scan scope, that Kaspersky Embedded Systems Security for Windows will apply in the On-Demand and Real-Time Computer Protection tasks.

- **Exploit Prevention**. You can protect process memory from exploits using a Protection Agent injected into the process.

Updates functionality (including providing anti-virus signature updates and codebase updates), as well as KSN functionality may not be available in the program in the U.S.

What's new

The new version of Kaspersky Embedded Systems Security for Windows introduces the following new features and improvements:

- The Device Control task has the following new expanded capabilities:
  - More types of devices can now be monitored. Added USB keyboards and USB mice, Bluetooth devices, SD card readers connected via USB or to the PCI bus.
  - Added the capability to specify multiple users or user groups with different levels of access to removable drives and SD card readers connected via USB or to the PCI bus.
- Added the Certificate Monitor component, which implements the functionality of notifications about untrusted signatures of applications and scripts being launched, as well as notifications about the approaching expiration date of signature certificates for applications and scripts.
- Implemented the capability to update password-protected Kaspersky Embedded Systems Security for Windows using the remote installation task of Kaspersky Security Center.
- A setting has been added to the Installation Wizard of application so that you can choose automatic installation of patches (if any) during installation or upgrade of the application.
- Added support for desktop operating systems: Windows 11 24H2 Home / Pro / Education / Enterprise.
- Added support for embedded operating systems: Windows 11 24H2 IoT Enterprise.
- Added support for server operating systems: Windows Server 2003 SP2 Standard / Enterprise, Windows Server 2003 R2 SP2 Standard / Enterprise, Windows Server 2008 SP2 Standard / Enterprise, Windows Server 2008 R2 SP1 Standard / Enterprise.
- It is forbidden to use certain characters to specify paths and file names when creating or editing Firewall rules.
- Expanded the list of application status parameters on the host, returned via the WMI API, with the following information: whether the logging of debug information is enabled and the name of the folder for saving trace files, whether the generation of memory dumps is enabled and the name of the folder for saving dump files.
- Added the display of information about integrated patches within the name of the installed application.
- When installing the application, you can exclude the Applications Launch Control component from the list of installation components.
- Issues from the previous versions are resolved: this application version includes fixes from earlier versions.

Sources of information about Kaspersky Embedded Systems Security for Windows

This section lists sources of information about the application.

You can select the most suitable information source, depending on the importance level and urgency of the issue.

Sources for independent retrieval of information

You can use the following sources to find information about Kaspersky Embedded Systems Security for Windows:

- Kaspersky Embedded Systems Security for Windows page on the Kaspersky website.
- Kaspersky Embedded Systems Security for Windows page on the Technical Support website (Knowledge Base).
- Manuals.

If you did not find a solution to your problem, contact Kaspersky Technical Support.

An Internet connection is required to use online information sources.

Kaspersky Embedded Systems Security for Windows page on the Kaspersky website

On the Kaspersky Embedded Systems Security for Windows page, you can review general information about the application and its functions and features.

The Kaspersky Embedded Systems Security for Windows page contains a link to the online store. There you can purchase the application or renew your license.

Kaspersky Embedded Systems Security for Windows page in the Knowledge Base

The Knowledge Base is a section of the Technical Support website.

On the Kaspersky Embedded Systems Security for Windows page in the Knowledge Base, you can find articles that provide useful information, recommendations, and answers to frequently asked questions about how to purchase, install, and use the application.

Knowledge Base articles can answer questions relating to not only Kaspersky Embedded Systems Security for Windows but also other Kaspersky applications. Knowledge Base articles can also include Technical Support news.

Kaspersky Embedded Systems Security for Windows documentation

The Kaspersky Embedded Systems Security for Windows Administrator's Guide contains information about installing, uninstalling, configuring, and using the application.

Discussing Kaspersky applications on the Forum

You can discuss questions related to Kaspersky applications with other users and Kaspersky experts on our Forum.

On the Forum, you can view existing topics, leave comments, and create new discussion topics.

Kaspersky Embedded Systems Security for Windows

This section describes the functions, components, and distribution kit of Kaspersky Embedded Systems Security for Windows, and provides a list of hardware and software requirements of Kaspersky Embedded Systems Security for Windows.

Distribution kit

The distribution kit includes the welcome application that lets you do the following:

- Start the Kaspersky Embedded Systems Security for Windows application Installation Wizard.
- Start the Kaspersky Embedded Systems Security for Windows Console Installation Wizard.
- Start the Installation Wizard, which will install Kaspersky Embedded Systems Security for Windows Administration Plug-in for managing the application via Kaspersky Security Center.
- Go to Kaspersky Embedded Systems Security for Windows page on the Kaspersky website.
- Visit the Technical Support website.
- Read information about the current version of Kaspersky Embedded Systems Security for Windows.

The distribution kit files are stored in the different folders depending on their intended use (see table below).

Kaspersky Embedded Systems Security for Windows distribution kit files

File	Purpose
autorun.inf	Autorun file for the Kaspersky Embedded Systems Security for Windows Installation Wizard when installing the application from removable drive.
release_notes.txt	The file contains release information.
migration.txt	The file describes migration from previous application versions.
setupui.exe	Greeting program start file (starts setup.hta).
ess.kud	File in Kaspersky Unicode Definition format with a description of the installation package for remote installation of application via Kaspersky Security Center.
\console\esstools.msi	Windows Installer package. Installs the Application Console on the managed device.
\console\setup.exe	Startup file for a wizard that installs a set of Administration Tools components (including the Kaspersky Embedded Systems Security for Windows Console). The installation package file esstools.msi is started with the installation settings specified in the wizard.
\console\license.txt	Kaspersky Embedded Systems Security for Windows Management Console End User License Agreement text file.
\exec\bases.cab	Archive of anti-virus databases current at the time of application release.
\exec\config.ini	Configuration file with installation parameters for creation of

	Kaspersky Embedded Systems Security for Windows installation package in Kaspersky Security Center.
\exec\ess.kud	File in Kaspersky Unicode Definition format with a description of the installation package for remote installation of Kaspersky Embedded Systems Security for Windows via Kaspersky Security Center.
\exec\ess_x64.msi	Windows Installer package. Installs the Kaspersky Embedded Systems Security for Windows on the managed device running a 64-bit Microsoft Windows operating system.
\exec\ess_x86.msi	Windows Installer package. Installs the Kaspersky Embedded Systems Security for Windows on the managed device running a 32-bit Microsoft Windows operating system.
\exec\klcfginst.exe	Installer for Administration Plug-in for managing application via Kaspersky Security Center.
\exec\license.txt	Kaspersky Embedded Systems Security for Windows End User License Agreement and Privacy Policy text file.
\exec\setup.exe	The file for installing Kaspersky Embedded Systems Security for Windows on the protected device via the wizard; it starts the installation package file ess.msi with the installation settings specified in the wizard.
\exec\disclaimer.txt	Patching disclaimer.
\product_long_term\config.ini	Configuration file with installation parameters for creation of Kaspersky Embedded Systems Security for Windows installation package in Kaspersky Security Center.
\product_long_term\ess_light.kud	File in Kaspersky Unicode Definition format with a description of the installation package for remote installation of Kaspersky Embedded Systems Security for Windows via Kaspersky Security Center.
\product_long_term\ess_x86.msi	Windows Installer package. Installs the Protect computer with Default Deny technology configuration of Kaspersky Embedded Systems Security for Windows on the protected computer running a 32-bit operating system.

	The components enabling updates are not included in the Protect computer with Default Deny technology configuration. If the Protect computer with Default Deny technology configuration is selected, the following components are included by default: • Core • Exploit Prevention • Applications Launch Control • System Tray Icon When you install the "Protect computer with Default Deny technology" configuration of application over an application version that uses signature analysis and anti-virus databases to protect your computer, the set of application components will be automatically reduced by removing the following components: • Real-Time File Protection • On-Demand Scan • the components enabling updates This configuration is recommended for protecting devices with limited resources. In this case, you can activate the application for a long term, and the Applications Launch Control component provides computer protection.
\product_long_term\ess_x64.msi	Windows Installer package. Installs the Protect computer with Default Deny technology configuration of Kaspersky Embedded Systems Security for Windows on the protected computer running a 64-bit operating system.

	The components enabling updates are not included in the Protect computer with Default Deny technology configuration. If the Protect computer with Default Deny technology configuration is selected, the following components are included by default: • Core • Exploit Prevention • Applications Launch Control • System Tray Icon When you install the "Protect computer with Default Deny technology" configuration of application over an application version that uses signature analysis and anti-virus databases to protect your computer, the set of application components will be automatically reduced by removing the following components: • Real-Time File Protection • On-Demand Scan • the components enabling updates This configuration is recommended for protecting devices with limited resources. In this case, you can activate the application for a long term, and the Applications Launch Control component provides computer protection.
\product_long_term\klcfginst.exe	Installer for Administration Plug-in for managing application via Kaspersky Security Center.
\product_long_term\license.txt	Kaspersky Embedded Systems Security for Windows End User License Agreement and Privacy Policy text file.
\product_long_term\setup.exe	The file for installing Kaspersky Embedded Systems Security for Windows on the protected device using the installation wizard; it starts the installation package file ess.msi with the installation settings specified in the wizard.
\product_long_term\disclaimer.txt	Patching disclaimer.
\setup\images	Folder with application welcome screen launch files.
\setup\setup.hta	Application welcome screen launch file.
\setup\SETUP_STRINGS.JS	File with the application string resources.

Software and hardware requirements

Before installing Kaspersky Embedded Systems Security for Windows, you must uninstall other anti-virus applications from the device.

Software requirements for the protected device

You can install Kaspersky Embedded Systems Security for Windows on a device running a 32-bit or 64-bit Microsoft Windows operating system.

Windows Installer 3.1 is required for proper installation and operation of the application on a protected device running Microsoft Windows XP.

To install and use Kaspersky Embedded Systems Security for Windows on protected devices with embedded operating systems, the Filter Manager component is required.

For correct operation of Kaspersky Embedded Systems Security for Windows, SHA-2 support is required in Windows. For detailed information, see: https://support.kaspersky.com/15728.

You can install Kaspersky Embedded Systems Security for Windows on a device running one of the following 32-bit or 64-bit Microsoft Windows operating systems:

- Workstations:
  - Windows XP Professional SP2 32-bit / 64-bit
  - Windows XP Professional SP3 32-bit
  - Windows 7 Home/Professional/Enterprise/Ultimate SP1 32-bit / 64-bit
  - Windows 8 Pro/Enterprise 32-bit / 64-bit
  - Windows 8.1 Pro/Enterprise 32-bit / 64-bit
  - Windows 10 version 1507 Home / Pro / Education / Enterprise 32-bit / 64-bit
  - Windows 10 LTSC 2015 version 1507 32-bit / 64-bit
  - Windows 10 RS1 version 1607 Home / Pro / Education / Enterprise 32-bit / 64-bit
  - Windows 10 LTSC 2016 version 1607 32-bit / 64-bit
  - Windows 10 RS2 version 1703 Home / Pro / Education / Enterprise 32-bit / 64-bit
  - Windows 10 RS3 version 1709 Home / Pro / Education / Enterprise 32-bit / 64-bit
  - Windows 10 RS4 version 1803 Home / Pro / Education / Enterprise 32-bit / 64-bit
  - Windows 10 RS5 version 1809 Home / Pro / Education / Enterprise 32-bit / 64-bit
  - Windows 10 LTSC 2019 version 1809 32-bit / 64-bit

- Windows 10 19H2 version 1909 Home / Pro / Education / Enterprise 32-bit / 64-bit
- Windows 10 21H2 version 21H2 Home / Pro / Education / Enterprise 32-bit / 64-bit
- Windows 10 LTSC 2021 version 21H2 32-bit / 64-bit
- Windows 10 22H2 version 22H2 Home / Pro / Education / Enterprise 32-bit / 64-bit
- Windows 11 21H2 version 21H2 Home / Pro / Education / Enterprise 64-bit
- Windows 11 22H2 version 2H2 Home / Pro / Education / Enterprise 64-bit
- Windows 11 23H2 version 23H2 Home / Pro / Education / Enterprise 64-bit
- Windows 11 24H2 version 24H2 Home / Pro / Education / Enterprise 64-bit

- Servers:
  - Windows Server 2003 SP2 Standard / Enterprise 32-bit / 64-bit
  - Windows Server 2003 R2 SP2 Standard / Enterprise 32-bit / 64-bit
  - Windows Server 2008 SP2 Standard / Enterprise 32-bit / 64-bit
  - Windows Server 2008 R2 SP1 Standard / Enterprise 64-bit
- Embedded systems:
  - Windows XP Embedded SP2 (WEPOS) 32-bit / 64-bit
  - Windows XP Embedded SP3 (POS Ready 2009) 32-bit
  - Windows 7 Embedded SP1 (POSReady 7) 32-bit / 64-bit
  - Windows 8.0 Embedded Industry Pro 32-bit / 64-bit
  - Windows 8.1 Embedded Industry Pro 32-bit / 64-bit
  - Windows 10 version 1507 IoT Enterprise 32-bit / 64-bit
  - Windows 10 version 1607 IoT Enterprise 32-bit / 64-bit
  - Windows 10 version 1703 IoT Enterprise 32-bit / 64-bit
  - Windows 10 version 1709 IoT Enterprise 32-bit / 64-bit
  - Windows 10 version 1803 IoT Enterprise 32-bit / 64-bit
  - Windows 10 version 1809 IoT Enterprise 32-bit / 64-bit
  - Windows 10 version 1909 IoT Enterprise 32-bit / 64-bit
  - Windows 10 version 21H2 IoT Enterprise 32-bit / 64-bit
  - Windows 10 version 22H2 IoT Enterprise 32-bit / 64-bit

- Windows 11 version 21H2 IoT Enterprise 64-bit
- Windows 11 version 22H2 IoT Enterprise 64-bit
- Windows 11 version 23H2 IoT Enterprise 64-bit
- Windows 11 version 24H2 IoT Enterprise 64-bit.

Supported versions of Kaspersky Security Center

Kaspersky Embedded Systems Security for Windows is compatible with the following versions of Kaspersky Security Center:

- Kaspersky Security Center Windows versions 10.5, 11. Management of Kaspersky Embedded Systems Security for Windows installed on computers running the Microsoft Windows XP SP2 operating system is supported via Administration Console using the Administration Plug-in and via Web Console using the Web Plug-in.
- Kaspersky Security Center Windows versions 13.2, 14.2. Management of Kaspersky Embedded Systems Security for Windows is supported via Administration Console using the Administration plug-in and via Web Console using the Web Plug-in.
- Kaspersky Security Center Linux versions 15, 15.1. Management of Kaspersky Embedded Systems Security for Windows via Web Console is supported using the Web Plug-in.

To manage Kaspersky Embedded Systems Security for Windows via Kaspersky Security Center, Kaspersky Security Center Network Agent is required.

Kaspersky Security Center Network Agent is not included in the Kaspersky Embedded Systems Security for Windows distribution kit. You can download it on the applications download page in the **Kaspersky Security Center** section.

Hardware requirements for the protected device

Hardware requirements for the protected device

OS type	OS name	Minimum requirements	Recommended requirements

Workstations	Windows XP x86 / x64	• Processor: 1.4 GHz single-core processor Pentium III (x32), Pentium IV (x64).
		• RAM:
		  • To install the Applications Launch Control component only – 256 MB.
		  • To install all application components – 512 MB
		• Free disk space:
		  • To install the Applications Launch Control component only – 50 MB.
			• Processor: 2.4 GHz quad-core
			• RAM: 2 GB
			• Free disk space:
			  • To install the Applications Launch Control component only – 2 GB.
			  • To install all application components – 4 GB

		• To install all application components – 2 GB	

	Windows 7 / 8 / 10 x86	• Processor: 1.4 GHz single-core processor Pentium III (x32), Pentium IV (x64).
		• RAM:
		  • To install the Applications Launch Control component only – 256 MB.
		  • To install all application components – 1 GB
		• Free disk space:
		  • To install the Applications Launch Control component only – 50 MB.
		  • To install all application components – 2 GB
			• Processor: 2.4 GHz quad-core
			• RAM: 2 GB
			• Free disk space:
			  • To install the Applications Launch Control component only – 2 GB.
			  • To install all application components – 4 GB

	Windows 7 / 8 / 10 / 11 x64	• Processor: 1.4 GHz single-core processor Pentium IV (x64).
		• RAM:
		  • To install the Applications Launch Control component only – 1 GB.
		  • To install all application components – 2 GB
		• Free disk space:
		  • To install the Applications Launch Control component only – 50 MB.
		  • To install all application components – 2 GB
			• Processor: 2.4 GHz quad-core
			• RAM:
			  • To install the Applications Launch Control component only – 2 GB.
			  • To install all application components – 4 GB
			• Free disk space:
			  • To install the Applications Launch Control component only – 2 GB.
			  • To install all application components – 4 GB

Server	Windows Server 2003 x86 / x64 Windows Server 2008 x86 / x64	• Processor: 1.4 GHz single-core processor Pentium IV (x64) or higher. • RAM: 512 MB • Free disk space: 4GB	• Processor: 2.4 GHz quad-core • RAM: 2 GB. • Free disk space: 4GB
Embedded	Windows XP		

	Embedded
	
	Windows Embedded POSReady 2009
		• Processor: 1.4 GHz single-core processor Pentium III (x32), Pentium IV (x64).
		• RAM:
		  • To install the Applications Launch Control component only – 256 MB.
		  • To install all application components – 512 MB
		• Free disk space:
		  • To install the Applications Launch Control component only – 50 MB.
		  • To install all application components – 2 GB
			• Processor: 2.4 GHz quad-core
			• RAM: 2 GB
			• Free disk space:
			  • To install the Applications Launch Control component only – 2 GB.
			  • To install all application components – 4 GB

	Windows 7 / 8 Embedded
	
	Windows 10 / 11 IoT
		• Processor: 1.4 GHz single-core processor Pentium IV (x64).
		• RAM: 1 GB.
		• Free disk space:
		  • To install the Applications Launch Control component only – 50 MB.
		  • To install all application components – 2 GB
			• Processor: 2.4 GHz quad-core
			• RAM: 2 GB
			• Free disk space:
			  • To install the Applications Launch Control component only – 2 GB.
			  • To install all application components – 4 GB

Limiting functionality on outdated Windows versions

- When creating an installation package in Kaspersky Security Center version 12 and later, to install Kaspersky Embedded Systems Security for Windows on devices running Windows XP or Windows Server 2003, you must use the setup.exe executable file from the installation package created in Kaspersky Security Center version 10.5.
- To manage Kaspersky Embedded Systems Security for Windows via Kaspersky Security Center:
  - on a computer running Windows XP SP2 Professional (32-bit/64-bit), Windows Server 2003 or Windows Server 2003 R2, you must use Kaspersky Security Center Network Agent (klnagent) version 10.5.1781.
  - on a computer running Windows XP SP3 Professional (32-bit) and Windows XP Embedded SP3 (32-bit), you must use Kaspersky Security Center Network Agent (klnagent) version 14.0.0.20023.

Functional requirements and limitations

This section describes additional functional requirements and existing limitations for Kaspersky Embedded Systems Security for Windows components.

Installation and uninstallation

Following is the list of installation and uninstallation limitations:

- For correct operation of Kaspersky Embedded Systems Security for Windows, SHA-2 support is required in Windows.
- When you install the application, a warning may appear on the screen If the specified path to the Kaspersky Embedded Systems Security for Windows installation folder contains more than 150 characters. The warning does not affect the installation process: you can install and run Kaspersky Embedded Systems Security for Windows.
- If you want to install the SNMP protocol support component, make sure to restart the SNMP service if the SNMP service is running.
- If you want to install and run Kaspersky Embedded Systems Security for Windows on a device running on an embedded operating system, make sure to install the Filter Manager component.
- You cannot install Kaspersky Embedded Systems Security for Windows Administration Tools via Microsoft Active Directory® group policies.
- If you exclude the Anti-virus Protection node from the list of installed application components, this node disappears from the list of available components after the installation is completed. To install the components of the Anti-virus Protection node, start the Installation Wizard from the installation package since the installation package contains a full list of components.
- If Kaspersky Embedded Systems Security for Windows Administration Console is installed, the Installation Wizard may prompt to restart the computer. In this case, reboot is not mandatory. It is sufficient to end the session of the user who installed the Administration Console and log in to the system again.
- If you install the application on the protected devices running on older operating systems unable to receive regular updates, ensure that the following root certificates are installed:
  - DigiCert Assured ID Root CA
  - DigiCert_High_Assurance_EV_Root_CA
  - DigiCertAssuredIDRootCA

  If the specified root certificates are not installed, the application may function improperly. We recommend that you install the certificates as soon as possible.

File Integrity Monitor

By default, the File Integrity Monitor does not monitor changes in the system folders or the file system's housekeeping files to not clutter task reports with information about routine file changes performed constantly by the operating system. You cannot include such folders in the monitoring scope.

The following folders and files are excluded from the monitoring scope:

- NTFS housekeeping files with file id from 0 to 33
- %SystemRoot%\Prefetch\
- %SystemRoot%\ServiceProfiles\LocalService\AppData\Local\
- %SystemRoot%\System32\LogFiles\Scm\
- %SystemRoot%\Microsoft.NET\Framework\v4.0.30319\
- %SystemRoot%\Microsoft.NET\Framework64\v4.0.30319\
- %SystemRoot%\Microsoft.NET\
- %SystemRoot%\System32\config\
- %SystemRoot%\Temp\
- %SystemRoot%\ServiceProfiles\LocalService\
- %SystemRoot%\System32\winevt\Logs\
- %SystemRoot%\System32\wbem\repository\
- %SystemRoot%\System32\wbem\Logs\
- %ProgramData%\Microsoft\Windows\WER\ReportQueue\
- %SystemRoot%\SoftwareDistribution\DataStore\
- %SystemRoot%\SoftwareDistribution\DataStore\Logs\
- %ProgramData%\Microsoft\\Windows\AppRepository\
- %ProgramData%\Microsoft\Search\\Data\Applications\Windows\
- %SystemRoot%\Logs\SystemRestore\
- %SystemRoot%\System32\Tasks\Microsoft\\Windows\TaskScheduler\

The application excludes top-level folders.

The component does not monitor files changes that bypass the ReFS/NTFS file system (file changes made through BIOS, LiveCD, and more).

Firewall Management

Following is the list of limitations for Firewall Management:

- You should specify more than one address. Otherwise, working with IPv6 is unavailable.
- Preset Firewall policy rules support basic scenarios of interaction between protected devices and Administration Server. To make full use of Kaspersky Security Center functions, you need to configure port

rules. You can find information about port numbers, protocols and their functions in the Kaspersky Security Center Knowledge Base.

- After the application is installed and rules for the task are configured, the application monitors changes to Windows Firewall rules and rule groups when the Firewall Management task is started. To update the status and add the required rules, make sure to restart the Firewall management task.

- When the Firewall Management task is started, denying rules and rules monitoring outgoing traffic are automatically removed from the operating system firewall settings.

- Characters "*" and "?" can not be used in the application path and in firewall rule name for application.

Other limitations

Limitations of **On-Demand Scan** and **Real-Time File Protection**:

- Scanning of connected MTP-devices is not available.

- Archive scanning is unavailable without SFX-archive scanning: if archive scanning is enabled in the protection settings of Kaspersky Embedded Systems Security for Windows, the application automatically scans objects in both archives and SFX-archives. SFX-archive scanning is available without archive scanning.

- If **Deeper analysis of launching processes (process launch is blocked until the analysis ends)** checkbox and **KSN Usage** are enabled simultaneously, any launched process that receives URL web-address as an argument will be blocked, even if Statistics only mode was chosen. To avoid blocking the process, please choose one of the options:

  - Disable **KSN Usage**.

  - Disable **Deeper analysis of launching processes (process launch is blocked until the analysis ends)** checkbox

  Recommended option: Disable Deeper analysis of launching processes checkbox

- When an attempt is made to run the On-Demand Scan task on a host without the On-Demand Scan component installed, the application displays a message about task execution internal error, rather than an explicit indication of the absence of the On-Demand Scan component.

Licensing:

- You cannot activate the application with a key via the Setup wizard if the key was created using the SUBST command, or if the path to the key file is a network path.

- If you plan to use a Kaspersky Security Center proxy server to activate the product on a client device, disable VDI optimization on that device when installing Kaspersky Security Center Network Agent.

Updates:

- By default, the application icon is hidden after Kaspersky Embedded Systems Security for Windows critical modules updates are installed.

- KLRAMDISK is not supported on protected devices running the Windows XP or Windows Server® 2003 operating system.

Interface:

- In the Application Console, filtering in the Quarantine, Backup, System audit log or Task log is case sensitive.
- When configuring a protection or scan scope in the Application Console, you can use only one mask and only at the end of the path. Following are the examples of correct masks: "C:\Temp\Temp*", or "C:\Temp\Temp???.doc", and "C:\Temp\Temp*.doc". This limitation does not affect configuration of the Trusted Zone.

Security:

- If the operating system's User Account Control feature is enabled, a user account must be part of the ESS Administrators group to be able to open the Application Console by double-clicking the application icon in the tray notification area. Otherwise, it will be necessary to login as a user who is allowed to open the Compact Diagnostic Interface or Microsoft Management Console snap-in.
- If User Account Control is enabled, you cannot uninstall the application via the Microsoft Windows Programs and Features window.

Integration with Kaspersky Security Center:

- When update packages are received, Administration Server verifies database updates before sending the updates to protected devices on the network. Administration Server does not verify software module updates.
- Make sure that the required check boxes are selected in the Interaction with the Administration Server settings when you use the components that transmit dynamic data to Kaspersky Security Center using network lists (Quarantine, Backup).

Exploit prevention:

- Exploit Prevention is unavailable if the apphelp.dll libraries are not loaded in the current environment configuration.
- The Exploit Prevention component is incompatible with the EMET utility from Microsoft on protected devices running the Microsoft Windows 10 operating system. Kaspersky Embedded Systems Security for Windows blocks EMET if the Exploit Prevention component is installed on a protected device with the EMET utility installed.
- The Exploit Prevention component is incompatible with the SQL Server® 2012 Database Engine. If you install Kaspersky Embedded Systems Security for Windows on the computer with installed MS SQL Server 2012, you must add the sqlos.dll library of the database server to the list of exclusions in the Exploit Prevention task.

Installing and removing the application

This section provides step-by-step instructions for installing and removing Kaspersky Embedded Systems Security for Windows.

About Kaspersky Embedded Systems Security for Windows update

An upgrade to Kaspersky Embedded Systems Security for Windows version 3.4 is available for application versions 2.3, 3.1, 3.2 and 3.3. To update from another version, remove the installed version and install version 3.4.

The update is performed by installing the new version of the application over the installed version of the application and does not require a computer restart.

By default, the application creates a new installation folder with the name of the new application version based on the path to the existing application installation folder. You can manually specify a new path for the application installation folder.

When upgrading Kaspersky Embedded Systems Security for Windows to version 3.4, the previously installed version of the application is automatically deleted.

If your version of Kaspersky Embedded Systems Security for Windows is earlier than 2.3, you must first uninstall the installed application before installing the new version.

When updating a password-protected installation of Kaspersky Embedded Systems Security for Windows version 2.3 or later, pass the password to the installer in one of the following ways:

- If installing locally via the Installation Wizard interface or in interactive CLI mode, specify the password when requested.
- If installing locally in non-interactive CLI mode, specify the password in the `UNLOCK_PASSWORD` key.
- If installing remotely via Kaspersky Security Center, pass the current password in the installation package settings.
- When installing application via Active Directory group policies, specify the value of UNLOCK PASSWORD key in the install_props.json configuration file.

When updating the application, the current license is automatically applied to Kaspersky Embedded Systems Security for Windows version 3.4, and the use of the new application components and tasks is fully available. The license term remains unchanged.

If an application is updated with an expired license, the new version of the application runs in limited functionality mode after installation (for example, application database updates are not available).

Migrating settings values of the updated application version

The following settings remain unchanged during application update:

- application and task settings
- task logs and system audit logs

- contents of Quarantine and Backup
- accounts under which tasks are started
- user access permissions for application management
- settings for notifications about the operation of tasks
- KAVFS service continues execution with PPL attribute if the attribute was assigned to it in the previous version of the application

The following settings are reset or changed to the default values for the new version of the application during application upgrade:

- all counters, including anti-virus database statuses
- data about installed updates of application modules and anti-virus databases
- task statuses
- application and task settings configured through the registry
- application and task settings that were changed during the installation of critical fixes.

Migrating the list of blocked network sessions

The list of blocked network sessions of client computers is not migrated during an application update.

The settings for automatically unblocking access to blocked network file resources remain unchanged during an application update.

Migrating Applications Launch Control settings and rules

During an application upgrade, Applications Launch Control rules are migrated without changes.

When updating the application, we recommend that you stop the Applications Launch Control task if it is running in active mode, or change the task to *Statistics only* mode.

After completing an update of the application, we recommend checking the migrated Applications Launch Control rules and their operation in *Statistics only* mode.

Migrating values of Firewall Management settings and rules

During an application upgrade, the rules for the Firewall Management task are migrated without changes.

If the Firewall Management component was not installed in a previous version of the application, after the application upgrade, the Firewall Management task runs in *Monitor Windows Firewall status* mode.

If the Firewall Management component was installed in a previous version of the application, the Firewall Management task runs in *Control Windows Firewall* mode after the application upgrade.

Updating the application with configuration modification

When you install the "Protect computer with Anti-Virus Bases" configuration of application from /exec folder over an application version that does not use signature analysis and anti-virus databases to protect your computer ("Protect computer with Default Deny technology"), the set of application components will be automatically expanded by adding the following components:

- Real-Time File Protection
- On-Demand Scan
- Network Threat Protection

The archive containing the anti-virus databases is unpacked automatically.

If you do not want to use these components and tasks to protect your device, restart the application installation from the /product_long_term folder.

When you install the "Protect computer with Default Deny technology" configuration of application from /product_long_term folder over an application version that uses signature analysis and anti-virus databases to protect your computer ("Protect computer with Anti-Virus Bases" configuration), the set of application components will be automatically reduced by removing the following components:

- Real-Time File Protection
- On-Demand Scan
- the components enabling updates

This configuration is recommended for protecting devices with limited resources. In this case, you can activate the application for a long term, and the Applications Launch Control component provides computer protection.

Kaspersky Security Network Statement and Kaspersky Managed Protection Statement

After application update to version 3.4, the KSN usage task is stopped. To continue usage of KSN cloud infrastructure and KMP Service after application update, you must read and accept the terms of Kaspersky Security Network Statement and Kaspersky Managed Protection Statement.

About Kaspersky Embedded Systems Security for Windows Administration Tools update

Any version of Application Console can be updated to Kaspersky Embedded Systems Security Console for Windows version 3.4.

Additionally:

- Settings values of the updated Application Console remain unchanged.
- Any previous version of Kaspersky Embedded Systems Security for Windows can be managed by Application Console version 3.4.
- Kaspersky Embedded Systems Security for Windows version 3.4 can be managed by Application Console of any previous version.

The following Administration Plug-in versions can be updated to version 3.4:

- 2.3.0.xxx;
- 3.1.0.xxx;
- 3.2.0.xxx.
- 3.3.0.xxx.

Additionally:

- The values of the Administration Plug-in settings of any afore mentioned versions remain unchanged after an upgrade to version 3.4.
- The following versions of Kaspersky Embedded Systems Security for Windows can be managed by Administration Plug-in version 3.4: 2.3.0.754, 3.1.0.461, 3.2.0.200, 3.3.0.87.
- Kaspersky Embedded Systems Security for Windows version 3.4 can be managed by Administration Plug-in of any of the afore mentioned versions.

During the update a new version of the Administration Plug-in or Application Console is installed over the previously installed version and does not require a computer restart.

Kaspersky Embedded Systems Security for Windows software component codes for the Windows Installer service

The \product_long_term\ess_x86.msi and \product_long_term\ess_x64.msi files are designed to install the Protect computer with Default Deny technology configuration of Kaspersky Embedded Systems Security for Windows, and the \product\ess_x86.msi and \product\ess_x64.msi files are designed to install the Protect computer with Anti-Virus Bases configuration of Kaspersky Embedded Systems Security for Windows.

If the "Protect computer with Anti-Virus Bases" configuration is selected, all Kaspersky Embedded Systems Security for Windows components are included by default except the Firewall Management and Performance Counters components.

When you install the "Protect computer with Anti-Virus Bases" configuration of application over an application version that does not use signature analysis and anti-virus databases to protect your computer, the set of application components will be automatically expanded by adding the following components:

- Real-Time File Protection
- On-Demand Scan
- Network Threat Protection

The components enabling updates are not included in the Protect computer with Default Deny technology configuration.

If the Protect computer with Default Deny technology configuration is selected, the following components are included by default:

- Core
- Exploit Prevention
- Applications Launch Control
- System Tray Icon

When you install the "Protect computer with Default Deny technology" configuration of application over an application version that uses signature analysis and anti-virus databases to protect your computer, the set of application components will be automatically reduced by removing the following components:

- Real-Time File Protection
- On-Demand Scan
- the components enabling updates

This configuration is recommended for protecting devices with limited resources. In this case, you can activate the application for a long term, and the Applications Launch Control component provides computer protection.

The \console\esstools_x86.msi and \console\esstools_x64.msi files install all software components that are part of the Administration Tools.

The following sections list the Kaspersky Embedded Systems Security for Windows component codes for the Windows Installer service. These codes can be used to define a list of components to be installed when installing Kaspersky Embedded Systems Security for Windows from the command line.

Kaspersky Embedded Systems Security for Windows software components

The following table contains codes and descriptions of Kaspersky Embedded Systems Security for Windows software components.

Description of Kaspersky Embedded Systems Security for Windows software components

Component	Identifier	Component functions
Basic functionality	Core	This component contains the set of basic application functions and ensures their operation. If other Kaspersky Embedded Systems Security for Windows components are specified when installing Kaspersky Embedded Systems Security for Windows from the command line, but the Core component is not specified, the Core component is installed automatically.
Applications Launch Control	AppCtrl	This component monitors user attempts to start applications and allows or denies application launch in accordance with specified Applications Launch Control rules.

		It is implemented in the Applications Launch Control task.
Device Control	DevCtrl	This component tracks attempts to connect external devices to a protected device and allows or denies use of these devices according to the specified device control rules. The component is implemented in the Device Control task.
Anti-Virus Protection	AVProtection	This component provides anti-virus protection.
Network Threat Protection	IDS	This component scans inbound network traffic for activity that is typical of network attacks. Upon detecting an attempted network attack that targets your computer, Kaspersky Embedded Systems Security for Windows blocks network activity from the attacking computer.
On-Demand Scan	Ods	This component installs Kaspersky Embedded Systems Security for Windows system files and performs On-Demand scan tasks (scanning of objects on the protected device upon request).
Real-Time File Protection	Oas	This component performs virus scans of files on the protected device when these files are accessed. It implements the Real-Time File Protection task.
Use of Kaspersky Security Network	Ksn	This component provides protection based on Kaspersky cloud technologies. It implements the KSN Usage task (sending requests to and receiving conclusions from the Kaspersky Security Network service).
File Integrity Monitor	Fim	This component logs operations performed on files in the specified monitoring scope. The component implements the File Integrity Monitor task.
Registry Access Monitor	RegMonitor	This component makes it possible to monitor actions performed with the specified registry branches and keys in the monitoring scopes defined in the task settings. The component implements the Registry Access Monitor.
Exploit Prevention	AntiExploit	This component makes it possible to manage settings to protect memory used by processes in a device's memory.
Firewall Management	Firewall	This component makes it possible to manage Windows Firewall through the Kaspersky Embedded Systems Security for Windows graphical user interface. The component implements the Firewall Management task.
Module for integration with Kaspersky Security Center Network Agent	AKIntegration	Provides a connection between the Kaspersky Embedded Systems Security for Windows and the Kaspersky Security Center Network Agent. You can install this component on the protected device if you intend to manage the application via Kaspersky Security Center.
Log Inspection	LogInspector	This component monitors the integrity of the protected environment based on the results of an inspection of Windows event logs.
Set of "System Monitor"	PerfMonCounters	This component installs a set of System Monitor performance counters. Performance counters enable Kaspersky Embedded Systems Security for Windows performance to be measured and

performance counters		potential bottlenecks to be located when Kaspersky Embedded Systems Security for Windows is used with other programs.
SNMP counters and traps	SnmpSupport	This component publishes Kaspersky Embedded Systems Security for Windows counters and traps via the Simple Network Management Protocol (SNMP) on Microsoft Windows. This component may be installed on the protected device only if Microsoft SNMP is installed on the same protected device.
Kaspersky Embedded Systems Security for Windows icon in the notification area	TrayApp	This component displays the Kaspersky Embedded Systems Security for Windows icon in the task tray notification area of the protected device. The Kaspersky Embedded Systems Security for Windows icon displays the status of device protection and can be used to open the Kaspersky Embedded Systems Security for Windows Console in Microsoft Management Console (if installed) and the **About the application** window.

"Administration tools" software component

The following table contains the code and the description of the "Administration tools" software component.

Description of the "Administration tools" software component

Component	Code	Component functions
Kaspersky Embedded Systems Security for Windows snap-in	MmcSnapin	This component installs the Microsoft Management Console snap-in to manage the application via the Kaspersky Embedded Systems Security for Windows Console. MmcSnapin is installed automatically; it does not need to be specified in the setup command parameters.

System changes after Kaspersky Embedded Systems Security for Windows installation

When Kaspersky Embedded Systems Security for Windows and the set of "Administration Tools" (including the Application Console) are installed together, the Windows Installer service will make the following modifications on the protected device:

- Kaspersky Embedded Systems Security for Windows folders are created on the protected device and on the device where the Application Console is installed.
- Kaspersky Embedded Systems Security for Windows services are registered.
- Kaspersky Embedded Systems Security for Windows user group is created.
- Kaspersky Embedded Systems Security for Windows keys are registered in the system registry.
- Kaspersky Embedded Systems Security OS Upgrade Detect system task that is displayed in the Windows Task Scheduler is created.

These changes are described below.

Kaspersky Embedded Systems Security for Windows folders on a protected device

When Kaspersky Embedded Systems Security for Windows is installed, the following folders are created on a protected device:

- Kaspersky Embedded Systems Security for Windows default installation folder containing the Kaspersky Embedded Systems Security for Windows executable files depend on the operating system bit set. Therefore, the default installation folders are as follows:
  - For the 32-bit version of Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security
  - On the 64-bit version of Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security
- Management Information Base (MIB) files containing a description of the counters and hooks published by Kaspersky Embedded Systems Security for Windows via the SNMP protocol:
  - %Kaspersky Embedded Systems Security%\mibs
- 64-bit versions of Kaspersky Embedded Systems Security for Windows executable files (this folder will be created only during installation of Kaspersky Embedded Systems Security for Windows on the 64-bit version of Microsoft Windows):
  - %Kaspersky Embedded Systems Security%\x64
- Kaspersky Embedded Systems Security for Windows service files:
  - %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.4\Data
  - %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.4\Settings
  - %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.4\Dskm

  For Windows XP the path to the Kaspersky Lab folder is %ALLUSERSPROFILE%\Application Data
- Files with settings for update sources:

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.4\Update

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.4\Update
- Updates of databases and software modules downloaded using the Copying Updates task (the folder will be created the first time updates are downloaded using the Copying Updates task).

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.4\Update\Distribution
- Task logs and system audit log.

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.4\Reports
- Set of databases currently in use.

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.4\Bases\Current
- Backup copies of databases; they are overwritten each time the databases are updated.

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.4\Bases\Backup

- Temporary files created during execution of update tasks.

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.4\Bases\Temp

- Quarantined objects (default folder).

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.4\Quarantine

- Objects in backup (default folder).

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.4\Backup

- Objects restored from backup and quarantine (default folder for restored objects).

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.4\Restored

Folder created during installation of Application Console

The Application Console default installation folders containing the "Administration Tools" files depend on the operating system bit set. Therefore, the default installation folders are as follows:

- For the 32-bit version of Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools

- For the 64-bit version of Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools

Kaspersky Embedded Systems Security for Windows services

The following Kaspersky Embedded Systems Security for Windows services start using the local system (SYSTEM) account:

- Kaspersky Security Service (KAVFS) – essential Kaspersky Embedded Systems Security for Windows service that manages Kaspersky Embedded Systems Security for Windows tasks and workflows.

- Kaspersky Security Management Service (KAVFSGT) – this service is intended for Kaspersky Embedded Systems Security for Windows application management through the Application Console.

- Kaspersky Security Exploit Prevention Service (KAVFSSLP) – this service acts as an intermediary to communicate security settings to external security agents, and to receive data about security events.

Kaspersky Embedded Systems Security for Windows group

ESS Administrators is a group on the protected device whose users have full access to the Kaspersky Security Management Service and all Kaspersky Embedded Systems Security functions.

System registry keys

When Kaspersky Embedded Systems Security for Windows is installed, the following system registry keys are created:

- Properties of the Kaspersky Embedded Systems Security for Windows: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]

- Kaspersky Embedded Systems Security for Windows event log settings (Kaspersky Event Log): [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security]
- Properties of the Kaspersky Embedded Systems Security for Windows management service: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]
- Performance counter settings:
  - For the 32-bit version of Microsoft Windows: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance]
  - For the 64-bit version of Microsoft Windows: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance]
- SNMP Protocol Support component settings:
  - For the 32-bit version of Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.4\SnmpAgent]
  - For the 64-bit version of Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.4\SnmpAgent]
- Dump file settings:
  - For the 32-bit version of Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.4\CrashDump]
  - For the 64-bit version of Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.4\CrashDump]
- Trace file settings:
  - For the 32-bit version of Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.4\Trace]
  - For the 64-bit version of Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.4\Trace]
- Settings for application tasks and functions: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.4\Environment]

Kaspersky Embedded Systems Security OS Upgrade Detect system task

The Windows Installer service creates a Kaspersky Embedded Systems Security OS Upgrade Detect task during application installation. The task is started immediately after it is created and later at every OS startup. The task checks the version of the drivers used by the application: if an operating system version is updated, the application updates the drivers for the corresponding version of the operating system.

The task does not affect the application and can be deleted. We recommend to keep operating system upgrade scenario in mind.

Kaspersky Embedded Systems Security for Windows processes

Kaspersky Embedded Systems Security for Windows starts processes described in the table below.

Kaspersky Embedded Systems Security for Windows processes

File name	Purpose
kavfswp.exe	Kaspersky Embedded Systems Security for Windows workflow
kavtray.exe	Process for the System Tray Icon
kavfsmui.exe	Process for the Compact Diagnostic Interface component
kavshell.exe	Command line utility process
kavfsrcn.exe	Kaspersky Embedded Systems Security for Windows remote management process
kavfs.exe	Kaspersky Security Service process
kavfsgt.exe	Kaspersky Security Management Service process
kavfswh.exe	Kaspersky Security Exploit Prevention Service process

Installation and recovery settings, and Windows Installer command-line options

This section describes the settings for installing Kaspersky Embedded Systems Security for Windows, the settings for uninstalling Kaspersky Embedded Systems Security for Windows, and the default options. The section also contains the keys for changing the installation settings and possible key values. These keys can be used in conjunction with standard keys for the Windows Installer service's `msiexec` command when installing Kaspersky Embedded Systems Security for Windows from the command line.

Installation settings and command line options in Windows Installer

- Acceptance of the terms of the End User License Agreement.

  The possible values for `EULA=<value>` command line option are as follows:

  - `0` – you reject the terms of the End User License Agreement (default value).
  - `1` – you accept the terms of the End User License Agreement.

- Acceptance of the terms of the Privacy Policy.

  The possible values for `PRIVACYPOLICY=<value>` command line option are as follows:

  - `0` – you reject the terms of the Privacy Policy (default value).
  - `1` – you accept the terms of the Privacy Policy.

- Consent to the provisions of the Disclaimer: you must accept the terms to install Kaspersky Embedded Systems Security for Windows patches if included in the distribution kit.

  DISCLAIMER=`<values>` can take the following values.

  - `0`: you reject the terms of the Disclaimer (default).
  - `1`: you accept the provisions of the Kaspersky Embedded Systems Security for Windows patching Disclaimer.

- Allow installation of Kaspersky Embedded Systems Security for Windows if the KB4528760 update not installed. For detailed information about the KB4528760 update please visit Microsoft website.

  The possible values for `SKIPCVEWINDOWS10=<value>` command line option are as follows:

  - `0` – cancel the installation of Kaspersky Embedded Systems Security for Windows if the KB4528760 update is not installed (default value).
  - `1` – allow the installation of Kaspersky Embedded Systems Security for Windows if the KB4528760 update is not installed.

  > The KB4528760 update fixes the CVE-2020-0601 security vulnerability. For detailed information about the CVE-2020-0601 security vulnerability please visit the Microsoft website.

- Installation of Kaspersky Embedded Systems Security for Windows with preservation of the settings of the previous version during the upgrade.

  The possible values for RESTOREDEFSETTINGS=<value> command line option are as follows:

  - `0` – All data from the previous version is migrated to the new version during the upgrade (default value).
  - `1` – Only the file with activation data and private keys is migrated to the new version during the upgrade ([drive]:\ProgramData\Kaspersky Lab\<product>\<version>\Data\product.dat). All other data from the previous version, such as settings, anti-virus databases, reports, quarantine and backup objects, are deleted.

- Installation of Kaspersky Embedded Systems Security for Windows with preservation of the reports from previous versions during the upgrade.

  The possible values for KEEP_REPORTS=<value> command line option are as follows:

  - `0` – all data from the previous version, except for reports ([drive]:\ProgramData\Kaspersky Lab\<product>\<version>\Reports), is migrated to the new version during the upgrade. The reports are deleted.
  - `1` – all data from the previous version, such as settings, anti-virus databases, reports, quarantine and backup objects, are migrated to the new version during the upgrade (default value).

- Installation of Kaspersky Embedded Systems Security for Windows with a preliminary scan of active processes and the boot sectors of local disks.

  The possible values for `PRESCAN=<value>` command line option are as follows:

  - `0` – do not perform a preliminary scan of active processes and the boot sectors of local disks during the installation (default value).
  - `1` – perform a preliminary scan of active processes and the boot sectors of local disks during the installation.

- Destination folder where Kaspersky Embedded Systems Security for Windows files will be saved during installation. A different folder can be specified.

  The default values for `INSTALLDIR=<full path to the folder>` command line option are as follows:

  - Kaspersky Embedded Systems Security for Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security
  - Administration tools: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools

- On the x64-bit version of Microsoft Windows: %ProgramFiles(x86)%

- Start of the Real-Time File Protection task immediately after Kaspersky Embedded Systems Security for Windows starts.

  The possible values for the `RUNRTP=< value >` command line option are:

  - `1` – start (default value).
  - `0` – do not start.

- Run mode for the Real-Time File Protection task.

  The possible values for the `RUNRTP=< value >` command line option are:

  - `1` – Recommended (default value).
  - `0` – Notify only.

- Objects excluded from the protection scope according to Microsoft Corporation recommendations. In the Real-Time File Protection task exclude from the protection scope objects on the device that Microsoft Corporation recommends to exclude. Some applications on the protected device may become unstable when an anti-virus application intercepts or modifies the files they use. For example, Microsoft Corporation includes some domain controller applications in the list of such objects.

  The possible values for `ADDMSEXCLUSION=<value>` command line option are as follows:

  - `1` – exclude (default value).
  - `0` – do not exclude.

- Objects excluded from the protection scope according to Kaspersky recommendations. In the Real-Time File Protection task exclude from the protection scope objects on the device that Kaspersky recommends to exclude.

  The possible values for `ADDKLEXCLUSION=<value>` command line option are as follows:

  - `1` – exclude (default value).
  - `0` – do not exclude.

- Connect to the Application Console remotely. By default, you cannot connect remotely to an Application Console installed on the protected device. During the installation, you can allow connection. Kaspersky Embedded Systems Security for Windows creates allowing rules for the process kavfsgt.exe using the TCP protocol for all ports.

  The possible values for `ALLOWREMOTECON=<value>` command line option are as follows:

  - `1` – allow.
  - `0` – deny (default value).

- Path to the key file (`LICENSEKEYPATH`). By default, the Windows Installer attempts to find the file with .key extension in the \exec folder of the distribution kit. If the \exec folder contains several key files, the Windows Installer will select the key file whose expiration date is the farthest into the future. A key file can be saved beforehand in the \exec folder or at another path that you can specify in the `LICENSEKEYPATH` parameter.

  `LICENSEKEYPATH` can take the following values.

  - Full path to the key file and key name.

- Path to the folder where key files are stored.

  You can add a key after Kaspersky Embedded Systems Security for Windows is installed using an administrative tool of your choice: for example, the Application Console. If you do not add a key during installation of the application, Kaspersky Embedded Systems Security for Windows will not function.

- Path to the configuration file. Kaspersky Embedded Systems Security for Windows imports settings from the specified configuration file created in the application. Kaspersky Embedded Systems Security for Windows does not import passwords from the configuration file, for example, account passwords for starting tasks, or passwords for connecting to a proxy server. Once the settings are imported, you will have to enter all passwords manually. If the configuration file is not specified, the application will start to work with the default settings after setup.

  The default value for `CONFIGPATH=<configuration file name>` is not specified.

- Scan at Operating System Startup mode (SCANSTARTUP_BLOCKING) If you install Kaspersky Embedded Systems Security for Windows in the install mode without the SCANSTARTUP_BLOCKING key, the Scan at Operating System Startup task has the following parameters assigned to the Scan scope setting:

  - Action to perform on infected and other objects: Notify only
  - Action to perform on probably infected objects: Notify only

  If you install Kaspersky Embedded Systems Security for Windows in the install mode using the SCANSTARTUP_BLOCKING key, the Scan at Operating System Startup task has the following parameters assigned to the Scan scope setting:

  - Action to perform on infected and other objects: Perform recommended action
  - Action to perform on probably infected objects: Perform recommended action

  A Scan at Operating System Startup task is created automatically. By default, the *Notify only* mode is applied. In this case, after you deploy Kaspersky Embedded Systems Security for Windows on the devices, you can enable the Scan at Operating System Startup task if no issues with system services were discovered during scan. If the application detects critical system services as infected or probably infected objects, the Notify only mode gives you time to figure out the reason and solve the issue. If the application is running in Perform Recommended Action mode, a *Disinfect* **action is performed.** *Remove, if disinfection fails* action. Disinfection or removal of the system files may result in critical issues with operating system startup.

- Enables network connections to manage Kaspersky Embedded Systems Security for Windows remotely from another device where the Application Console is installed. Port 135 (TCP) is opened in Microsoft Windows Firewall, network connections are allowed for the executable file kavfsrcn.exe for remote management of Kaspersky Embedded Systems Security for Windows, and access is granted to DCOM applications. When installation is complete, add users to the ESS Administrators group to let them remotely manage the application, and allow network connections to the Kaspersky Security Management Service (kavfsgt.exe file) on the protected device. You can read more about additional configuration when the Kaspersky Embedded Systems Security for Windows Console is installed on another device.

  The possible values for `ADDWFEXCLUSION=<value>` command line option are as follows:

  - `1` – allow.
  - `0` – deny (default value).

- Disabling the check for incompatible software. Use this setting to enable or disable the check for incompatible software during background installation of the application on the protected device. Regardless of the value of this setting, during installation of Kaspersky Embedded Systems Security for Windows, the application always warns about other versions of the application installed on the protected device.

  The possible values for `SKIPINCOMPATIBLESW=<value>` command line option are as follows:

- `0` – The check for incompatible software is performed (default value).
- `1` – The check for incompatible software is not performed.

- Set up individual application components: `ADDLOCAL=<semicolon-delimited application component codes>`.
- Register Kaspersky Security as a protected process using the ELAM driver.

  The `NOPPL=<value>` command-line option can take the following values.

  - `0`: Kaspersky Security service is registered in the operating system as a protected process.
  - `1`: Kaspersky Security service is not registered in the operating system as a protected process.
- Enables/disables Kaspersky Security Center Network Agent (klnagent) power saving mode.

  `SKIP_KLNAG_FLAG_TEST_VM_PERF=<value>` can take the following values.

  - `0`: after the Kaspersky Embedded Systems Security for Windows setup is complete, Kaspersky Security Center Network Agent (klnagent) will run in power saving mode—no information about local users will be sent to the Kaspersky Security Center server. You will be able to specify local users in the Kaspersky Embedded Systems Security for Windows policies and tasks settings only manually, and you will not be able to use the Kaspersky Security Center Administration Server list for this.
  - `1`: after Kaspersky Embedded Systems Security for Windows installation is complete, Kaspersky Security Center Network Agent (klnagent) will send information about local users to the Kaspersky Security Center server. You will be able to specify local users in the Kaspersky Embedded Systems Security for Windows policies and tasks settings manually or with the help of the Kaspersky Security Center Administration Server list.

  A `SKIP_KLNAG_FLAG_TEST_VM_PERF=<value>` command-line option is not specified, which corresponds to a `SKIP_KLNAG_FLAG_TEST_VM_PERF=0` command-line option.

Recovery settings and Windows Installer command-line options

- Restoring quarantined objects.

  The possible values for `RESTOREQTN=<value>` command line option are as follows:

  - `0` – Remove quarantined content (default value).
  - `1` – Restore quarantined content to the folder specified by the RESTOREPATH parameter into the \Quarantine subfolder.
- Restoring the content of backup.

  The possible values for `RESTOREBCK=<value>` command line option are as follows:

  - `0` – Remove backup content (default value).
  - `1` – Restore backup contents to the folder specified by the RESTOREPATH parameter into the \Backup subfolder.
- Enter the current password to confirm the uninstallation (if password protection is enabled).

  The default value for `UNLOCK_PASSWORD=<specified password>` is not specified.

- Folder for restored objects. Restored objects will be saved to the specified folder.

  The default value for the `RESTOREPATH=<full path to the folder>` command line option is %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\3.4\Restored

- Remove individual application components: `ADDLOCAL=<semicolon-delimited application component codes>`.

Kaspersky Embedded Systems Security for Windows install and uninstall logs

If Kaspersky Embedded Systems Security for Windows is installed or uninstalled using the Installation (Uninstallation) Wizard, the Windows Installer service creates an install (uninstall) log. A log file named ess_v3.4_install_<uid>.log (where <uid> is a unique 8-character log identifier) will be saved in the %temp% folder for the user whose account was used to start the setup.exe file.

If you run the **Modify or Remove** option for the Application Console or Kaspersky Embedded Systems Security for Windows from the **Start** menu, a log file named ess_v3.4_install_<uid> is automatically created in the %temp% folder.

If Kaspersky Embedded Systems Security for Windows is installed or uninstalled from the command line, the install log file will not be created by default.

To install Kaspersky Embedded Systems Security for Windows and create a log file on disk C:\:

- `msiexec /i ess_x86.msi /l*v C:\ess.log /qn EULA=1 PRIVACYPOLICY=1`
- `msiexec /i ess_x64.msi /l*v C:\ess.log /qn EULA=1 PRIVACYPOLICY=1`

Installation planning

This section describes the set of Kaspersky Embedded Systems Security for Windows administration tools, and special aspects of installing and uninstalling Kaspersky Embedded Systems Security for Windows using a wizard, command line, using Kaspersky Security Center and via an Active Directory group policy.

Before starting installation of Kaspersky Embedded Systems Security for Windows, plan the main stages of the installation.

1. Determine which administration tools will be used to manage and configure Kaspersky Embedded Systems Security for Windows.
2. Select the necessary application components for installation.
3. Select the installation method.

Selecting administration tools

Determine the administration tools that will be used to configure Kaspersky Embedded Systems Security for Windows settings and to manage the application. Kaspersky Embedded Systems Security for Windows can be managed using the Application Console, command-line utility, and Kaspersky Security Center Administration Console.

Kaspersky Embedded Systems Security for Windows Console

Kaspersky Embedded Systems Security for Windows Console is a standalone snap-in added to the Microsoft Management Console. Kaspersky Embedded Systems Security for Windows can be managed via the Application Console installed on the protected device or on another device on the corporate network.

Multiple Kaspersky Embedded Systems Security for Windows snap-ins can be added to one Microsoft Management Console opened in author mode to use it to manage the protection of multiple device with Kaspersky Embedded Systems Security for Windows installed.

The Application Console is included in the set of "Administration Tools" application components.

Command line utility

You can manage Kaspersky Embedded Systems Security for Windows from the command line of a protected device.

The command line utility is included in the Kaspersky Embedded Systems Security for Windows software components group.

Kaspersky Security Center

If Kaspersky Security Center is used for centralized management of anti-virus protection of devices at your company, you can manage Kaspersky Embedded Systems Security for Windows via the Kaspersky Security Center Administration Console.

The following components must be installed:

- **Module for integration with Kaspersky Security Center Network Agent**. This component is included in the Kaspersky Embedded Systems Security for Windows software components group. It allows Kaspersky Embedded Systems Security for Windows to communicate with the Network Agent. Install the module for integration with Kaspersky Security Center Network Agent on the protected device.

- **Kaspersky Security Center Network Agent**. Install this component on each protected device. This component supports interaction between Kaspersky Embedded Systems Security for Windows installed on the protected device and Kaspersky Security Center Administration Console. The Network Agent installation file is included in the Kaspersky Security Center distribution kit folder.

- **Kaspersky Embedded Systems Security 3.4 for Windows Administration Plug-in**. Additionally, install the Administration Plug-in for managing Kaspersky Embedded Systems Security for Windows via the Administration Console on the protected device where the Kaspersky Security Center Administration Server is installed. This provides the interface for application management via Kaspersky Security Center. The Administration Plug-in installation file, \exec\klcfginst.exe, is included in the Kaspersky Embedded Systems Security for Windows distribution kit.

Selecting the installation type

After specifying the software components for installation of Kaspersky Embedded Systems Security for Windows, you need to select the application installation method.

Select the installation method depending on the network architecture and the following conditions:

- Whether you need special Kaspersky Embedded Systems Security for Windows installation settings, or the recommended installation settings.
- Whether the installation settings will be the same for all protected devices or specific to each protected device.

Kaspersky Embedded Systems Security for Windows can be installed interactively using the Setup Wizard or in silent mode without user involvement, and can be invoked by running the installation package file with installation settings from the command line. A centralized remote installation of Kaspersky Embedded Systems Security for Windows can be performed using Active Directory group policies or using the Kaspersky Security Center remote installation task.

Kaspersky Embedded Systems Security for Windows can be installed and configured on a single protected device with its settings saved to a configuration file; the file can then be used to install Kaspersky Embedded Systems Security for Windows on other protected devices. Note that this ability does not exist when the application is installed using Active Directory group policies.

Starting the Setup Wizard

The Setup Wizard can install the following:

- Kaspersky Embedded Systems Security for Windows components on the protected device, by clicking the link in the welcome application, which can be started by opening setupui.exe or directly using \exec\setup.exe file in the distribution kit.
- Kaspersky Embedded Systems Security for Windows Console on the protected device or other device on the LAN, by clicking the link in the welcome application, which can be started by opening setupui.exe or directly using \console\setup.exe file in the distribution kit.

Running the installation package file from the command line with the necessary installation settings

If the installation package file is started without command-line options, Kaspersky Embedded Systems Security for Windows will be installed with the default settings. Kaspersky Embedded Systems Security for Windows options can be used to modify the installation settings.

The Application Console can be installed on the protected device and / or administrator's workstation.

You can also use sample commands for the installation of Kaspersky Embedded Systems Security for Windows and the Application Console.

Centralized installation via Kaspersky Security Center

If Kaspersky Security Center is used in your network for managing networked devices' anti-virus protection, Kaspersky Embedded Systems Security for Windows can be installed on multiple devices by using the remote installation task.

The protected devices on which you want to install Kaspersky Embedded Systems Security for Windows using Kaspersky Security Center may be in the same domain as Kaspersky Security Center in a different domain, or in no domain at all.

Centralized installation using Active Directory group policies

Active Directory group policies can be used to install Kaspersky Embedded Systems Security for Windows on the protected device. The Application Console can be installed on the protected device or administrator's workstation.

Kaspersky Embedded Systems Security for Windows can be installed using just the recommended installation settings.

The protected devices on which Kaspersky Embedded Systems Security for Windows is installed using Active Directory group policies must be located in the same domain and the same organizational unit. Installation is performed at protected device start before logging in to Microsoft Windows.

Installing and uninstalling the application using a wizard

This section describes the installation and uninstallation of Kaspersky Embedded Systems Security for Windows and the Application Console by means of the Setup Wizard, and contains information about additional configuration of Kaspersky Embedded Systems Security for Windows and actions to be performed upon installation.

Installing using the Setup Wizard

The following sections contain information about installation of Kaspersky Embedded Systems Security for Windows and the Application Console.

To install and proceed to use Kaspersky Embedded Systems Security for Windows:

1. Install Kaspersky Embedded Systems Security for Windows on the protected device.
2. Install the Application Console on the devices from which you intend to manage Kaspersky Embedded Systems Security for Windows.
3. If the Application Console has been installed on any device in the network other than the protected device, perform additional configuration to allow Application Console users to manage Kaspersky Embedded Systems Security for Windows remotely.
4. Perform actions after installation of Kaspersky Embedded Systems Security for Windows.

Kaspersky Embedded Systems Security for Windows installation

Before installing Kaspersky Embedded Systems Security for Windows, do the following:

1. Make sure no other anti-virus programs are installed on the protected device.
2. Make sure that the account you use to run the Setup Wizard belongs to the administrators group on the protected device.

After completing the actions described above, proceed with the installation procedure. Following the Setup Wizard instructions, specify the installation settings for Kaspersky Embedded Systems Security for Windows. The Kaspersky Embedded Systems Security for Windows installation process can be stopped at any step of the Setup Wizard. To do so, click the **Cancel** button in the Setup Wizard window.

You can read more about the installation (uninstallation) settings.

To install Kaspersky Embedded Systems Security for Windows using the Setup Wizard:

1. Run the setupui.exe file on the protected device.
2. In the window that opens, in the **Installation** section, click the **Protect computer with Default Deny technology** link or **Protect computer with Anti-Virus Bases** link.

   If the "Protect computer with Anti-Virus Bases" configuration is selected, all Kaspersky Embedded Systems Security for Windows components are included by default except the Firewall Management and Performance Counters components.

   When you install the "Protect computer with Anti-Virus Bases" configuration of application over an application version that does not use signature analysis and anti-virus databases to protect your computer, the set of application components will be automatically expanded by adding the following components:

   - Real-Time File Protection
   - On-Demand Scan
   - Network Threat Protection

   The components enabling updates are not included in the Protect computer with Default Deny technology configuration.

   If the Protect computer with Default Deny technology configuration is selected, the following components are included by default:

   - Core
   - Exploit Prevention
   - Applications Launch Control
   - System Tray Icon

   When you install the "Protect computer with Default Deny technology" configuration of application over an application version that uses signature analysis and anti-virus databases to protect your computer, the set of application components will be automatically reduced by removing the following components:

   - Real-Time File Protection
   - On-Demand Scan
   - the components enabling updates

   This configuration is recommended for protecting devices with limited resources. In this case, you can activate the application for a long term, and the Applications Launch Control component provides computer protection.

3. In the welcome screen of the Kaspersky Embedded Systems Security for Windows Setup Wizard, click the **Next** button.

   The **End User License Agreement and Privacy Policy** window opens.

4. Review the terms of the License Agreement and Privacy Policy.

5. If you agree to the terms and conditions of End User License Agreement and Privacy Policy, select the **I confirm that I have fully read, understood, and accept the terms and conditions of this End User License Agreement** and **I am aware and agree that my data will be handled and transmitted (including to third countries) as described in the Privacy Policy. I confirm that I have fully read and understand the Privacy Policy** check boxes in order to proceed with the installation.

   If you do not accept the End User License Agreement and/or Privacy Policy the installation will be aborted.

6. Click the **Next** button.

   If the distribution kit contains patches, a **Limited warranty Statement** window opens.

7. Please read the Disclaimer. This is a requirement for subsequent patching.

8. If you accept the terms of the Disclaimer, select **I confirm that I have fully read, understand, and accept the terms and conditions of this Limited warranty Statement** check box.

9. Click the **Next** button.

   The **Custom installation** window opens.

10. Select the components to be installed.

    The SNMP Protocol Support component of Kaspersky Embedded Systems Security for Windows will only appear in the list of components suggested for installation if the Microsoft Windows SNMP service is installed on the protected device.

11. To cancel all changes, click the **Custom installation** button in the **Reset** window.

12. Click the **Next** button.

13. In the **Select a destination folder** window:

    - If required, specify a folder to which Kaspersky Embedded Systems Security for Windows files will be copied.
    - If required, review the information about available space on local drives by clicking the **Disk** button.

    Click the **Next** button.

14. In the **Advanced installation settings** window, configure Real-Time File Protection.

15. Click the **Next** button.

16. To import Kaspersky Embedded Systems Security for Windows settings from an existing configuration file created in a compatible earlier version of the application, specify the path to the configuration file in the **Import settings from configuration file** window.

17. Click the **Next** button.

18. In the **Activation of the application** window, do one of the following:

    - If you want to activate the application, specify a Kaspersky Embedded Systems Security for Windows key file for application activation.
    - If you want to activate the application later, click the **Next** button.
    - If a key file was previously saved in the \exec folder of the distribution kit, the name of this file will be displayed in the **Key** field.

      To add a key using a key file stored in another folder, specify the key file.

      Once the key file is added, license information will be shown in the window. Kaspersky Embedded Systems Security for Windows displays the license's calculated expiration date. The license term runs from the time when you add a key and expires no later than the expiration date of the key file.

19. Click the **Next** button to apply the key file in the application.

20. In the **Ready to install** window, click the **Install** button.

    The wizard will start the installation of Kaspersky Embedded Systems Security for Windows components.

21. The **Installation complete** window opens when installation is complete.

22. Click the **Finish** button.

The Setup Wizard closes. Once installation is complete, Kaspersky Embedded Systems Security for Windows is ready to use if you have added an activation key.

Kaspersky Embedded Systems Security for Windows Console installation

Follow the instructions of the Setup Wizard to configure installation settings for the Application Console. The installation process can be stopped at any step of the wizard. To do so, click the **Cancel** button in the Setup Wizard window.

To install the Application Console:

1. Make sure that the account you use to run the Setup Wizard belongs to the administrators group on the device.

2. Run the setupui.exe file on the protected device.

   The welcome window opens.

3. Click on the **Install Kaspersky Embedded Systems Security for Windows Console** link.

   The Setup Wizard's welcome window opens.

4. Click the **Next** button.

5. In the window that opens, review the terms of the End User License Agreement and Privacy Policy, and select the check boxes under the **I confirm that I have fully read, understood, and accept the terms and conditions of this End User License Agreement** caption in order to proceed with the installation.

6. Click the **Next** button.

The **Advanced installation settings** window opens.

7. In the **Advanced installation settings** window:

   - If you intend to use the Application Console to manage Kaspersky Embedded Systems Security for Windows installed on a remote device, select the **Allow remote access** check box.
   - To open the **Custom installation** window and select components:

     a. Click the **Advanced** button.

     The **Custom installation** window opens.

     b. Select the "Administration Tools" components from the list.

     By default, all the components are installed.

     c. Click the **Next** button.

   You can find more detailed information about Kaspersky Embedded Systems Security for Windows components.

8. In the **Select a destination folder** window:

   a. If required, specify a different folder to which the files being installed should be saved.

   b. Click the **Next** button.

9. In the **Ready to install** window, click the **Install** button.

   The wizard will begin installing the selected components.

10. Click the **Finish** button.

The Setup Wizard closes. The Application Console will be installed on the protected device.

If Administration Tools has been installed on any device in the network other than protected device, configure the advanced settings.

Advanced settings after installation of the Application Console on another device

If the Application Console has been installed on any device in the network, other than a protected device, perform the following actions to allow users to manage Kaspersky Embedded Systems Security for Windows remotely:

- Add Kaspersky Embedded Systems Security for Windows users to the ESS Administrators group on the protected device.
- Allow network connections for the Kaspersky Security Management Service (kavfsgt.exe), if the protected device uses Windows Firewall or a third-party firewall.
- If the **Allow remote access** check box is not selected during installation of the Application Console on a device running Microsoft Windows, manually allow network connections for the Application Console via the device's firewall.

The Application Console on the remote device uses the DCOM protocol to receive information about Kaspersky Embedded Systems Security for Windows events (such as objects scanned, tasks completed, etc.) from the Kaspersky Security Management Service on the protected device. You need to allow network connections for the Application Console in the Windows Firewall settings in order to establish connections between the Application Console and the Kaspersky Security Management Service.

On the remote device, where the Application Console is installed, do the following:

- Make sure that anonymous remote access to COM applications is allowed (but not remote start and activation of COM applications).
- In Windows Firewall, open TCP port 135 and allow network connections for kavfsrcn.exe, the executable file of the Kaspersky Embedded Systems Security for Windows remote management process.

  The device where the Application Console is installed uses TCP port 135 to access the protected device and to receive a response.
- Configure an outbound rule for Windows Firewall to allow the connection.

  Unlike the traditional TCP/IP and UDP/IP services where a single protocol has a fixed port, DCOM dynamically assigns ports to remote COM objects. If a firewall exists between the client (where the Application Console is installed) and the DCOM endpoint (the protected device), a large range of ports must be opened.

The same steps should be applied to configure any other software or hardware firewall.

If the Application Console is open while you configure the connection between the protected device and the device on which the Application Console is installed:

1. Close the Application Console.
2. Wait until the Kaspersky Embedded Systems Security for Windows remote management process kavfsrcn.exe is finished.
3. Restart the Application Console.

   The new connection settings will be applied.

Allowing anonymous remote access to COM applications

The names of settings may vary depending on the installed Windows operating system.

To allow anonymous remote access to COM applications:

1. On the remote device with the Kaspersky Embedded Systems Security for Windows Console installed, open the Component Services console.
2. Select **Start** → **Run**.
3. Enter the command `dcomcnfg`.
4. Click the **OK** button.
5. Expand the **Computers** node in the **Component Services** console on your protected device.

6. Open the context menu on the **My Computer** node.
7. Select **Properties**.
8. On the **COM Security** tab of the **Properties** window, click the **Edit Limits** button in the **Access permissions** settings group.
9. Make sure that the **Allow Remote Access** check box is selected for the ANONYMOUS LOGON user in the **Allow Remote Access** window.
10. Click the **OK** button.

Allowing network connections for the Kaspersky Embedded Systems Security for Windows remote management process

The names of settings may vary depending on the installed Windows operating system.

To open TCP port 135 in Windows Firewall and to allow network connections for the Kaspersky Embedded Systems Security for Windows remote management process:

1. Close the Kaspersky Embedded Systems Security for Windows Console on the remote device.
2. Do one of the following:
   - On Microsoft Windows XP SP2 or later:
     a. Select **Start** > **Windows Firewall**.
     b. In the **Windows Firewall** window (or Windows Firewall settings), click the **Add port** button on the **Exclusions** tab.
     c. In the **Name** field, specify the port name RPC (TCP/135) or enter another name, for example Kaspersky Embedded Systems Security for Windows DCOM, and specify the port number (135) in the **Port name** field.
     d. Select the **TCP** protocol.
     e. Click the **OK** button.
     f. Click the **Add** button on the **Exclusions** tab.
   - On Microsoft Windows 7 or later:
     a. Select **Start** > **Control Panel** > **Windows Firewall**.
     b. In the **Windows Firewall** window, select **Allow a program or feature through Windows Firewall**.
     c. In the **Allow programs to communicate through Windows Firewall** window click the **Allow another program** button.
3. Specify the kavfsrcn.exe file in the **Add Program** window. It is located in the destination folder specified during installation of Kaspersky Embedded Systems Security for Windows Console using Microsoft Management

Console.

4. Click the **OK** button.
5. Click the **OK** button in the **Windows Firewall (Windows Firewall settings)** window.

Adding outbound rule for Windows Firewall

The names of settings may vary depending on the installed Windows operating system.

To add the outbound rule for Windows Firewall:

1. Select **Start** > **Control Panel** > **Windows Firewall**.
2. In the **Windows Firewall** window, click the **Advanced settings** link.
   The **Windows Firewall with Advanced Security** window opens.
3. Select the **Outbound Rules** child node.
4. Click the **New Rule** option in the **Actions** pane.
5. In the **New Outbound Rule Wizard** window that opens, select the **Port** option and click **Next**.
6. Select the **TCP** protocol.
7. In the **Specific remote ports** field specify the following ports range for allowing outgoing connections: 1024-65535.
8. In the **Action** window, select the **Allow the connection** option.
9. Save the new rule and close the **Windows Firewall with Advanced Security** window.

The Windows Firewall will now allow network connections between the Application Console and Kaspersky Security Management Service.

Actions to perform after Kaspersky Embedded Systems Security for Windows installation

Kaspersky Embedded Systems Security for Windows starts protection and scan tasks immediately after installation if you have activated the application. If **Enable Real-Time File Protection after installation of application (recommended)** (default option) is selected during installation of Kaspersky Embedded Systems Security for Windows, the application scans the device's file system objects when they are accessed. Kaspersky Embedded Systems Security for Windows will run the Critical Areas Scan task every Friday at 8:00 P.M.

We recommend that you take the following steps after installing Kaspersky Embedded Systems Security for Windows:

- Start the application database update task. After installation Kaspersky Embedded Systems Security for Windows will scan objects using the database included in the application distribution kit.

We recommend updating Kaspersky Embedded Systems Security for Windows databases immediately since they may be out of date.

The application will then update the databases every hour according to the default schedule configured in the task.

- Run a Critical Areas Scan of the device if no anti-virus software with real-time file protection was installed on the device before installation of Kaspersky Embedded Systems Security for Windows.
- Configure administrator notifications about Kaspersky Embedded Systems Security for Windows events.

Starting and configuring Kaspersky Embedded Systems Security for Windows Database Update task

To update the application database after installation:

1. In the Database Update task settings, configure a connection to an update source – Kaspersky HTTP or FTP update servers.
2. Start the Database Update task.

Web Proxy Auto-Discovery Protocol (WPAD) may not be configured on your network to detect proxy server settings automatically in the LAN. At that, your network may require authentication when accessing the proxy server.

To specify the optional proxy server settings and authentication settings for accessing the proxy server:

1. Open the context menu of the **Kaspersky Embedded Systems Security for Windows** node.
2. Select **Properties**.

   The **Application settings** window is displayed.
3. Select the **Connection settings** tab.
4. In the **Proxy server settings** section, select the **Use the specified proxy server** check box.
5. Enter the proxy server address in the **Address** field, and enter the port number for the proxy server in the **Port** field.
6. In the **Proxy server authentication settings** section, select the necessary authentication method in the drop-down list:
   - **Use NTLM authentication**, if the proxy server supports the built-in Microsoft Windows NTLM authentication. Kaspersky Embedded Systems Security for Windows will use the account specified in the task settings to access the proxy server. By default, the task is started under the **Local System** (**SYSTEM**) account.
   - **Use NTLM authentication with user name and password**, if the proxy server supports the built-in Microsoft Windows NTLM authentication. Kaspersky Embedded Systems Security for Windows will use the specified account to access the proxy server. Enter a user name and password or select a user from the list.

- **Apply user name and password**, to select basic authentication. Enter a user name and password or select a user from the list.

7. Click the **OK** button in the **Application settings** window.

To configure the connection to Kaspersky's update servers, in the Database Update task:

1. Start Application Console in one of the following ways:

   - Open the Application Console on the protected device. To do this, select **Start** > **All Programs** > **Kaspersky Embedded Systems Security for Windows** > **Administration Tools** > **Kaspersky Embedded Systems Security 3.4 for Windows Console**.

   - If the Application Console has been started on a device other than the protected one, connect to the device:

     a. Open the context menu of the **Kaspersky Embedded Systems Security for Windows** node in the Application Console tree.

     b. Select the **Connect to another computer** item.

     c. In the **Select protected device** dialog, select **Another device** and in the text field indicate the network name of the protected device.

     If the account you used to sign in to Microsoft Windows does not have access permissions for the Kaspersky Security Management Service, indicate an account with the required permissions.

   The Application Console window opens.

2. In the Application Console tree, expand the **Update** node.

3. Select the **Database Update** child node.

4. Click the **Properties** link in the results pane.

5. In the **Task settings** window that opens, open the **Connection settings** tab.

6. Select **Use proxy server settings to connect to Kaspersky update servers**.

7. Click the **OK** button in the **Task settings** window.

The settings for connecting to the update source in the Database Update task will be saved.

To run the Database Update task:

1. In the Application Console tree, expand the **Update** node.

2. In the context menu on the **Database Update** child node, select the **Start** item.

The Database Update task starts.

After the task has successfully completed, you can view the release date of the latest database updates installed in the results pane of the **Kaspersky Embedded Systems Security for Windows** node.

Critical Areas Scan

After you have updated the Kaspersky Embedded Systems Security for Windows databases, scan the protected device for malware using the Critical Areas Scan task.

To run the Critical Areas Scan task:

1. Expand the **On-Demand Scan** node in the Application Console tree.
2. In the context menu of the **Critical Areas Scan** child node, select the **Start** command.

The task starts; the **Running** task status is displayed in the results pane.

To view the task log,

in the results pane of the **Critical Areas Scan** node, click the **Open task log** link.

Modifying the set of components and repairing Kaspersky Embedded Systems Security for Windows

Kaspersky Embedded Systems Security for Windows components can be added or removed. You need to stop the Real-Time File Protection task before you can remove the Real-Time File Protection component. In other circumstances there is no need to stop the Real-Time File Protection task or Kaspersky Security Service.

If application management is password protected, Kaspersky Embedded Systems Security for Windows requests the password when you attempt to remove components or modify the set of components in the Setup Wizard.

To modify the set of Kaspersky Embedded Systems Security for Windows components:

1. In the **Start** menu, select **All programs** > **Kaspersky Embedded Systems Security for Windows** > **Modify or Remove Kaspersky Embedded Systems Security for Windows**.

   The Setup Wizard's **Modify, repair or remove installation** window opens.

2. Select **Modify components set**. Click the **Next** button.

   The **Custom installation** window opens.

3. In the **Custom installation** window, in the list of available components, select the components that you want to add or remove from Kaspersky Embedded Systems Security for Windows. To do this, perform the following actions:

   - To change the set of components, click the button next to the name of the selected component. Then in the context menu, select:
     - **Component will be installed on local hard drive**, if you want to install one component;
     - **Component and its subcomponents will be installed on local hard drive**, if you want to install a group of components.

- To remove previously installed components, click the button next to the name of the selected component. Then in the context menu, select **Component will be unavailable**.

Click the **Next** button.

4. In the **Ready to install** window, confirm the change to the set of software components by clicking the **Install** button.
5. In the window that opens when installation is complete, click the **OK** button.

The set of Kaspersky Embedded Systems Security for Windows components will be modified based on the specified settings.

If problems occur during the operation of Kaspersky Embedded Systems Security for Windows (Kaspersky Embedded Systems Security for Windows crashes; tasks crash or do not start), you can perform a repair for Kaspersky Embedded Systems Security for Windows. You can perform a repair while saving the current Kaspersky Embedded Systems Security for Windows settings, or you can select an option to reset all Kaspersky Embedded Systems Security for Windows settings to their default values.

To repair Kaspersky Embedded Systems Security for Windows after the application or a task crashes:

1. In the **Start** menu, select **All programs**.
2. Select **Kaspersky Embedded Systems Security for Windows**.
3. Select **Modify or Remove Kaspersky Embedded Systems Security for Windows**.

   The Setup Wizard's **Modify, repair or remove installation** window opens.
4. Select **Repair installed components**. Click the **Next** button.

   This opens the **Repair installed components** window.
5. In the **Repair installed components** window, select the **Restore recommended application settings** check box if you want to reset the application settings and restore Kaspersky Embedded Systems Security for Windows with its default settings. Click the **Next** button.
6. In the **Ready to repair** window, confirm the repair operation by clicking the **Install** button.
7. In the window that opens when the repair operation is complete, click the **OK** button.

Kaspersky Embedded Systems Security for Windows will be repaired using the specified settings.

Uninstalling using the Setup Wizard

This section contains instructions on removing Kaspersky Embedded Systems Security for Windows and the Application Console from a protected device using the Setup / Uninstallation Wizard.

Kaspersky Embedded Systems Security for Windows uninstallation

Dump and trace files are not deleted on uninstalling Kaspersky Embedded Systems Security for Windows. You can manually delete dump and trace files from the folder specified during the configuration of dump and trace files writing.

The names of settings may vary depending on the installed Windows operating system.

Kaspersky Embedded Systems Security for Windows can be uninstalled from the protected device using the Setup / Uninstallation Wizard.

After uninstalling Kaspersky Embedded Systems Security for Windows from a protected device a restart may be required. The restart can be postponed.

Uninstallation, repair and installation of the application is not available via the Windows Control Panel if the operating system uses the UAC feature (User Account Control) or access to the application is password protected.

If application management is password protected, Kaspersky Embedded Systems Security for Windows requests the password when you attempt to remove components or modify the set of components in the Setup Wizard.

To uninstall Kaspersky Embedded Systems Security for Windows:

1. In the **Start** menu, select **All programs**.
2. Select **Kaspersky Embedded Systems Security for Windows**.
3. Select **Modify or Remove Kaspersky Embedded Systems Security for Windows**.

   The Setup Wizard's **Modify, repair or remove installation** window opens.
4. Select **Remove software components**. Click the **Next** button.

   The **Advanced application uninstallation settings** window opens.
5. If necessary, in the **Advanced application uninstallation settings** window:

   a. Select the **Export quarantine objects** check box to make Kaspersky Embedded Systems Security for Windows export objects that have been quarantined. By default, the check box is cleared.

   b. Check the **Export Backup objects** check box to export objects from Kaspersky Embedded Systems Security for Windows Backup. By default, the check box is cleared.

   c. Click the **Save to** button and select the folder to which you want to export the objects. By default, the objects will be exported to %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\Uninstall.

   Click the **Next** button.
6. In the **Ready to uninstall** window, confirm the uninstallation by clicking the **Uninstall** button.
7. In the window that opens when the uninstallation is complete, click the **OK** button.

Kaspersky Embedded Systems Security for Windows will be uninstalled from the protected device.

Kaspersky Embedded Systems Security for Windows Console uninstallation

The names of settings may vary depending on the installed Windows operating system.

You can uninstall the Application Console from the protected device using the Setup / Uninstallation Wizard.

After uninstalling the Application Console, you do not need to restart the protected device.

To uninstall the Application Console:

1. In the **Start** menu, select **All programs**.
2. Select **Kaspersky Embedded Systems Security for Windows**.
3. Select **Modify or Remove Kaspersky Embedded Systems Security for Windows**.
   The wizard's **Repair or remove installation** window opens.
4. Select **Remove software components** and click the **Next** button.
5. The **Ready to uninstall** window opens. Click the **Uninstall** button.
   The **Uninstallation complete** window opens.
6. Click the **OK** button.

Uninstallation is now complete, and the Setup Wizard closes.

Installing and uninstalling the application from the command line

This section describes the particulars of installing and uninstalling Kaspersky Embedded Systems Security for Windows from the command line and contains examples of commands to install and uninstall Kaspersky Embedded Systems Security for Windows from the command line, and examples of commands to add and remove Kaspersky Embedded Systems Security for Windows components from the command line.

About installing and uninstalling Kaspersky Embedded Systems Security for Windows from command line

Dump and trace files are not deleted on uninstalling Kaspersky Embedded Systems Security for Windows. You can manually delete dump and trace files from the folder specified during the configuration of dump and trace files writing.

You can install or uninstall Kaspersky Embedded Systems Security for Windows and add or remove its components by running the \exec\ess_x86.msi or \exec\ess_x64.msi installation package file from the command line after you specify the installation settings using command-line options.

The "Administration Tools" set can be installed on the protected device or on another device on the network to work with the Application Console locally or remotely. To do this, use the \console\esstools.msi installation package.

Perform the installation using an account included in the administrators group on the protected device where the application is installed.

If the \exec\ess_x86.msi or \exec\ess_x64.msi file is run on the protected device without additional command-line options, Kaspersky Embedded Systems Security for Windows will be installed with the default installation settings.

You can assign the set of components to be installed using the ADDLOCAL command-line option and listing the codes for the selected components or sets of components.

Example commands for installing Kaspersky Embedded Systems Security for Windows

This section provides examples of commands used to install Kaspersky Embedded Systems Security for Windows.

On protected devices running a 32-bit version of Microsoft Windows, run the files with the x86 suffix in the distribution kit. On protected devices running a 64-bit version of Microsoft Windows, run the files with the x64 suffix in the distribution kit.

Detailed information about the use of Windows Installer's standard commands and command-line options is provided in the documentation supplied by Microsoft.

If you do not accept the End User License Agreement and Privacy Policy (default values `EULA=0` and `PRIVACYPOLICY=0`) the installation will not be completed.

Examples of installing Kaspersky Embedded Systems Security for Windows from the setup.exe file

To install Kaspersky Embedded Systems Security for Windows with the recommended installation settings and included patches, and without user involvement:

```
\exec\setup.exe /s /p EULA=1 /p PRIVACYPOLICY=1 DISCLAIMER=1
```

To install components, such as Device Control:

```
\exec\setup.exe /p ADDLOCAL=DevCtrl /p RUNRTP=0 /p ADDMSEXCLUSION=0
```

When installing Kaspersky Embedded Systems Security for Windows on computers with network devices and SCSI devices that cause a system crash after installation of application, the following additional options can be used with this command:

`/p SKIP_NETWORK_UPPERFILTERS=<1|0>`

Enables (1) or disables (0) interception of connections of network adapters.

`/p SKIP_SCSIADAPTER_UPPERFILTERS=<1|0>`

Enables (1) or disables (0) interception of connections of SCSI adapters.

List of commands used for installation: running an .msi file

To install Kaspersky Embedded Systems Security for Windows with the recommended installation settings without user involvement:

```
msiexec /i ess_x64(or x86).msi /qn EULA=1 PRIVACYPOLICY=1
```

To install Kaspersky Embedded Systems Security for Windows with the recommended installation settings and display the installation interface:

```
msiexec /i ess_x64(or x86).msi /qn EULA=1 PRIVACYPOLICY=1
```

To install Kaspersky Embedded Systems Security for Windows with the recommended installation settings and enable trace file rotation when the number of trace files reaches the specified maximum number:

```
msiexec /i ess_x64(or x86).msi TRACE_FOLDER=C:\Traces TRACE_MAX_ROLL_COUNT=50 /qn
EULA=1 PRIVACYPOLICY=1
```

The `TRACE_FOLDER` parameter is required.

The following rules apply to the `TRACE_MAX_ROLL_COUNT` parameter:

- If this parameter is specified, trace file rotation is enabled when the number of trace files reaches the maximum number specified in the parameter. Available range of parameters values: from 1 to 999.
- If the maximum number of trace files is specified as 0, trace file rotation is disabled.
- If a parameter value is specified, but is invalid or outside the range of available values (from 1 to 999), trace file rotation is enabled with the default maximum number of trace files set to 5.
- If the parameter is not specified:
  - If trace file rotation is already configured on the device, its settings are not changed. The application will ignore the entered parameters.
  - If trace file rotation is not configured on the device, the rotation option will be enabled with the default maximum number of trace files set to 5.

To install and activate Kaspersky Embedded Systems Security for Windows using the key file C:\0000000A.key:

```
msiexec /i ess_x64(or x86).msi LICENSEKEYPATH=C:\0000000A.key /qn EULA=1
PRIVACYPOLICY=1
```

To install Kaspersky Embedded Systems Security for Windows with a preliminary scan of active processes and the boot sectors of local disks:

```
msiexec /i ess_x64(or x86).msi PRESCAN=1 /qn EULA=1 PRIVACYPOLICY=1
```

To install Kaspersky Embedded Systems Security for Windows in the installation folder C:\ESS:

```
msiexec /i ess_x64(or x86).msi INSTALLDIR=C:\ESS /qn EULA=1 PRIVACYPOLICY=1
```

To install Kaspersky Embedded Systems Security for Windows and save an installation log file named ess.log in the folder where the Kaspersky Embedded Systems Security for Windows msi file is stored:

```
msiexec /i ess_x64(or x86).msi /l*v ess.log /qn EULA=1 PRIVACYPOLICY=1
```

To install Kaspersky Embedded Systems Security for Windows Console:

```
msiexec /i esstools.msi /qn EULA=1
```

To install and activate Kaspersky Embedded Systems Security for Windows using the key file C:\0000000A.key and configure Kaspersky Embedded Systems Security for Windows according to the settings in the configuration file C:\settings.xml:

```
msiexec /i ess_x64(or x86).msi LICENSEKEYPATH=C:\0000000A.key
CONFIGPATH=C:\settings.xml /qn EULA=1 PRIVACYPOLICY=1
```

To install an application patch when Kaspersky Embedded Systems Security for Windows is password-protected:

```
msiexec /p "<msp file name with path>" UNLOCK_PASSWORD=<password>
```

Actions to perform after Kaspersky Embedded Systems Security for Windows installation

Kaspersky Embedded Systems Security for Windows starts protection and scan tasks immediately after installation if you have activated the application. If you select the **Enable Real-Time File Protection after installation of application (recommended)** option during installation of Kaspersky Embedded Systems Security for Windows, the application scans the device's file system objects when they are accessed. Kaspersky Embedded Systems Security for Windows will run the Critical Areas Scan task every Friday at 8:00 P.M.

We recommend that you take the following steps after installing Kaspersky Embedded Systems Security for Windows:

- Start the Kaspersky Embedded Systems Security for Windows Database Update task. After installation Kaspersky Embedded Systems Security for Windows will scan objects using the database included in its distribution kit. We recommend that you update the Kaspersky Embedded Systems Security for Windows database immediately. To do so, you must run the Database Update task. The database will then be updated every hour according to the default schedule.

  For example, you can start the Database Update task by running the following command:

  ```
  KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser
  /PROXYPWD:123456
  ```

  In this case, Kaspersky Embedded Systems Security for Windows database updates are downloaded from Kaspersky update servers. Connection to an update source is established via a proxy server (proxy server address: proxy.company.com, port: 8080) using built-in Windows NTLM authentication to access the server under an account (user name: inetuser; password: 123456).

- Run a Critical Areas Scan of the device if no anti-virus software with real-time file protection was installed on the device before installation of Kaspersky Embedded Systems Security for Windows.

To start the Critical Areas Scan task using the command line:

```
KAVSHELL SCANCRITICAL /W:scancritical.log
```

This command saves the task log in a file named scancritical.log contained in the current folder.

- Configure administrator notifications about Kaspersky Embedded Systems Security for Windows events.

Adding / removing components. Sample commands

The Applications Launch Control component is installed automatically.

To install the On-Demand Scan component, run the following command:

```
msiexec /i ess.msi ADDLOCAL=Oas,Ods /qn
```

or

```
\exec\setup.exe /s /p ADDLOCAL=Oas,Ods
```

After you add the components to the list, Kaspersky Embedded Systems Security for Windows reinstalls the existing components and installs the specified components.

To remove installed components run the following command:

```
msiexec /i ess.msi REMOVE=Firewall,PerfMonCounters EULA=1 PRIVACYPOLICY=1 /qn
```

To install new components, run the following command:

```
msiexec /i ess.msi
ADDLOCAL=AKIntegration,AVProtection,AntiExploit,AppCtrl,DevCtrl,Fim,Ksn,LogInspector,Oas
EULA=1 PRIVACYPOLICY=1 /qn
```

After you list the components that you want to install and remove, Kaspersky Embedded Systems Security for Windows installs and removes the corresponding components.

Kaspersky Embedded Systems Security for Windows uninstallation. Sample commands

To uninstall Kaspersky Embedded Systems Security for Windows from the protected device, run the following command:

- For 32-bit operating systems:
  ```
  msiexec /x ess_x86.msi /qn
  ```
- For 64-bit operating systems:
  ```
  msiexec /x ess_x64.msi /qn
  ```

or

- For 32-bit operating systems:
  ```
  msiexec /x {A9FCA39D-B6D8-49B2-B65B-5751DDE4B47A} /qn
  ```
- For 64-bit operating systems:

```
msiexec /x {C73EA50B-F327-4DB0-82C7-FC83035EE66B} /qn
```

To uninstall Kaspersky Embedded Systems Security for Windows Console, run the following command:

```
msiexec /x esstools.msi /qn
```

or

```
msiexec /x {D9779DB9-91D6-46D0-84D2-ACC3781EC0DB} /qn
```

To uninstall Kaspersky Embedded Systems Security for Windows from a device on which password protection is enabled, perform the following command:

- For 32-bit operating systems:
  ```
  msiexec /x {A9FCA39D-B6D8-49B2-B65B-5751DDE4B47A} UNLOCK_PASSWORD=*** /qn
  ```
- For 64-bit operating systems:
  ```
  msiexec /x {C73EA50B-F327-4DB0-82C7-FC83035EE66B} UNLOCK_PASSWORD=*** /qn
  ```

Return codes

The table below contains a list of command-line return codes.

Return codes

Code	Description
1324	The destination folder name contains invalid characters.
25001	Insufficient rights to install Kaspersky Embedded Systems Security for Windows. To install the application, start the installation wizard with local administrator rights.
25003	Kaspersky Embedded Systems Security for Windows cannot be installed on devices running this version of Microsoft Windows. Please start the installation wizard for 64-bit versions of Microsoft Windows.
25004	Incompatible software detected. To continue the installation, uninstall the following software: <list of incompatible software>.
25010	The indicated path cannot be used to save quarantined objects.
25011	The name of the folder for saving quarantined objects contains invalid characters.
26251	Unable to download the Performance Counters DLL.
26252	Unable to download the Performance Counters DLL.
27300	The driver cannot be installed.
27301	The driver cannot be uninstalled.
27302	The network component cannot be installed. Maximum supported number of filtered devices reached.
27303	Anti-virus databases not found.

Installing and uninstalling the application using Kaspersky Security Center

This section contains information about installing Kaspersky Embedded Systems Security for Windows using Kaspersky Security Center, a description of the procedure for installing and uninstalling Kaspersky Embedded Systems Security for Windows through Kaspersky Security Center, and a description of actions to be taken after Kaspersky Embedded Systems Security for Windows is installed.

General information about installing via Kaspersky Security Center

You can install Kaspersky Embedded Systems Security for Windows via Kaspersky Security Center using the remote installation task.

After the remote installation task is complete, Kaspersky Embedded Systems Security for Windows will be installed with identical settings on multiple protected devices.

All protected devices can be combined in a single administration group, and a group task can be created to install Kaspersky Embedded Systems Security for Windows on the protected devices in this group.

You can create a task to remotely install Kaspersky Embedded Systems Security for Windows on a set of protected devices that are not in the same administration group. When creating this task, you must generate the list of individual protected devices that Kaspersky Embedded Systems Security for Windows should be installed on.

Detailed information on the remote installation task is provided in *Kaspersky Security Center Help*.

Rights to install or uninstall Kaspersky Embedded Systems Security for Windows

The account specified in the remote installation (removal) task must be included in the administrators group on each of the protected devices in all cases except those described below:

- If the Kaspersky Security Center Network Agent is already installed on the protected devices on which Kaspersky Embedded Systems Security for Windows is to be installed (regardless of which domain the protected devices are in or whether they belong to any domain).

  If the Network Agent is not yet installed on the protected devices, you can install it with Kaspersky Embedded Systems Security for Windows using a remote installation task. Before installing the Network Agent, make sure that the account you want to specify in the task is included in the administrators group on each of the protected devices.

- All protected devices on which you want to install Kaspersky Embedded Systems Security for Windows are in the same domain as the Administration Server, and the Administration Server is registered as the **Domain Admin** account (if this account has local administrator rights on the protected devices within the domain).

By default, when using the **Forced installation** method, the remote installation task is run from the account running the Administration Server.

When working with group tasks or with tasks for sets of protected devices under forced installation (uninstallation) mode, an account must have the following rights on the protected device:

- Right to execute applications remotely.
- Rights to the **Admin$** share.

- Right to **Log on as a service**.

Installing Kaspersky Embedded Systems Security for Windows via Kaspersky Security Center

Detailed information about generating an installation package and creating a remote installation task is provided in the Kaspersky Security Center Implementation Guide.

If you intend to manage Kaspersky Embedded Systems Security for Windows via Kaspersky Security Center in the future, make sure that the following conditions are met:

- The protected device where the Kaspersky Security Center Administration Server is installed also has the Administration Plug-in installed (\exec\klcfginst.exe file in the Kaspersky Embedded Systems Security for Windows distribution kit).
- Kaspersky Security Center Network Agent is installed on protected devices. If Kaspersky Security Center Network Agent is not installed on protected devices, you can install it together with Kaspersky Embedded Systems Security for Windows using a remote installation task.

Devices can also be combined into an administration group in order to later manage the protection settings using Kaspersky Security Center policies and group tasks.

To install Kaspersky Embedded Systems Security for Windows using a remote installation task via Kaspersky Security Center:

1. In the Kaspersky Security Center Administration Console expand the **Advanced** node.
2. Expand the **Remote installation** child node.
3. In the results pane of the **Installation packages** child node, click the **Create installation package** button.
4. Select the **Create installation package for a Kaspersky application** installation package type.
5. Enter the new installation package name.
6. Specify the ess.kud file located in Kaspersky Embedded Systems Security for Windows distribution kit \exec folder as the installation package file.

   The **End User License Agreement and Privacy Policy** window opens.
7. If you agree to the terms and conditions of End User License Agreement and Privacy Policy, select the **I confirm that I have fully read, understood, and accept the terms and conditions of this End User License Agreement** and **I am aware and agree that my data will be handled and transmitted (including to third countries) as described in the Privacy Policy. I confirm that I have fully read and understand the Privacy Policy** check boxes in order to proceed with the installation.

   You must accept the License Agreement and the Privacy Policy to proceed.
8. To change the set of Kaspersky Embedded Systems Security for Windows components to be installed and the default installation settings in the installation package:

a. In Kaspersky Security Center, expand the **Remote installation** node.

b. In the results pane of the **Installation packages** child node, open the context menu of the created Kaspersky Embedded Systems Security for Windows installation package and select **Properties**.

c. In the **Properties: <name of installation package>** window open the **Settings** section.

d. In the **Components to install** settings group, select the check boxes next to the names of the Kaspersky Embedded Systems Security for Windows components you want to install.

e. If necessary, change the run mode for Real-Time File Protection:

1. Click the button to the right of the **Real-Time File Protection** check box.
2. In the **Selecting security level** window, select the required option from the **Security level** drop-down list.

f. To automatically install patches if included in the application distribution kit:

1. Click **About limited warranty**.

   The **Limited warranty Statement** window opens.
2. Please read the Disclaimer.
3. If you accept the terms of the Disclaimer, select **I confirm that I have fully read, understand, and accept the terms and conditions of this Limited warranty Statement** check box.
4. Click the **OK** button.
5. In the installation package settings section, select **Automatically install patches** check box.

g. In order to indicate a destination folder other than the default one, specify the folder name and path in the **Destination folder** field.

> The path to the destination folder may contain system environment variables. If the folder does not exist on the protected device, it will be created.

h. In the **Advanced installation settings** group, configure the following settings:

- Scan protected device for viruses before installation.
- **Enable real-time protection after installation of application**.
- **Add Microsoft recommended files to exclusions list**.
- **Add Kaspersky recommended files to exclusions list**.
- **Make KSC Agent use less resources.**
- **Perform the recommended action during the scan at OS startup**.

i. To import Kaspersky Embedded Systems Security for Windows settings from an existing configuration file created in a compatible earlier version of the application, specify the path to the configuration file in the **Configuration file** field.

j. In the **Properties: <name of installation package>** window, click **OK**.

9. In the **Installation packages** node create a task to remotely install Kaspersky Embedded Systems Security for Windows on the selected protected devices (administration group).

10. Configure the Kaspersky Embedded Systems Security for Windows remote installation task.

    To learn more about creating and configuring remote installation tasks, see the *Kaspersky Security Center Help*.

11. Run the Kaspersky Embedded Systems Security for Windows remote installation task.

Kaspersky Embedded Systems Security for Windows will be installed on the protected devices specified in the task.

Actions to perform after Kaspersky Embedded Systems Security for Windows installation

After you install Kaspersky Embedded Systems Security for Windows, we recommend that you update Kaspersky Embedded Systems Security for Windows databases on the devices, and perform a Critical Areas Scan of the devices if no anti-virus applications with enabled real-time protection were installed on the devices before installation of Kaspersky Embedded Systems Security for Windows.

If the protected devices on which Kaspersky Embedded Systems Security for Windows was installed are part of the same administration group in the Kaspersky Security Center, you can perform these tasks using the following methods:

1. Create Database Update tasks for the group of protected devices on which Kaspersky Embedded Systems Security for Windows was installed. Set the Kaspersky Security Center Administration Server as the update source.

2. Create an On-Demand Scan group task with the Critical Areas Scan status. Kaspersky Security Center evaluates the security status of each protected device in the group based on the results of this task, not based on the results of the Critical Areas Scan task.

3. Create a new policy for the group of protected devices. In the policy properties, in the **Application settings** section, deactivate the scheduled start of local system on-demand scan tasks and the Database Update tasks on the administration group's protected devices in the settings of the **Run local system tasks** subsection.

You can also configure administrator notifications about Kaspersky Embedded Systems Security for Windows events.

Installing the Application Console via Kaspersky Security Center

Detailed information about creating an installation package and a remote installation task is provided in the Kaspersky Security Center Implementation Guide.

To install the Application Console using a remote installation task:

1. In the Kaspersky Security Center Administration Console expand the **Advanced** node.

2. Expand the **Remote installation** child node.

3. Create an installation package:

   a. In the results pane of the **Installation packages** child node, click the **Create installation package** button.

   b. In the **New Package Wizard** window, select **Create installation package for specified executable file** as a package type.

   c. Enter the new installation package name.

   d. Select the \console\setup.exe file from the Kaspersky Embedded Systems Security for Windows distribution kit folder and select the **Copy entire folder to the installation package** check box.

   e. In the **Executable file launch settings (optional)** field, set EULA=1. Otherwise, it is impossible to install components.

   ```
   /s /p "EULA=1"
   ```

   f. If necessary, in the **Executable file launch settings (optional)** field, you can specify the ADDLOCAL command-line parameter to change the set of components to be installed, and the INSTALLDIR command-line parameter to specify a destination folder other than the default one. For example, to perform a standalone installation of the Application Console in the C:\KasperskyConsole folder, use the following command-line option:

   ```
   /s /p "INSTALLDIR=C:\KasperskyConsole EULA=1"
   ```

4. In the **Installation packages** child node, create a task to remotely install the Application Console on the selected protected devices (administration group).

5. Configure the task settings.

   To learn more about creating and configuring remote installation tasks, see the Kaspersky Security Center Help.

6. Run the remote installation task.

The Application Console is installed on the protected devices specified in the task.

Uninstalling Kaspersky Embedded Systems Security for Windows via Kaspersky Security Center

Dump and trace files are not deleted on uninstalling Kaspersky Embedded Systems Security for Windows. You can manually delete dump and trace files from the folder specified during the configuration of dump and trace files writing.

If management of Kaspersky Embedded Systems Security for Windows on network devices is password protected, enter the password when creating a task to uninstall multiple applications. If the password protection is not managed centrally by a Kaspersky Security Center policy, Kaspersky Embedded Systems Security for Windows will be successfully uninstalled from the devices, on which the entered password matched the set value. Kaspersky Embedded Systems Security for Windows will not be uninstalled from other protected devices.

To uninstall Kaspersky Embedded Systems Security for Windows:

1. In the Kaspersky Security Center Administration Console, create and start an application removal task.

2. In the task, select the uninstallation method (similar to selecting the installation method; see the previous section) and specify the account that Administration Server will use to access the protected devices. You can uninstall Kaspersky Embedded Systems Security for Windows with only the default uninstallation settings.

Installing and uninstalling via Active Directory group policies

This section describes how to install and uninstall Kaspersky Embedded Systems Security for Windows through Active Directory group policies, as well as information on the actions that must be performed after installing Kaspersky Embedded Systems Security for Windows through group policies.

Installing Kaspersky Embedded Systems Security for Windows via Active Directory group policies

You can install Kaspersky Embedded Systems Security for Windows on several protected devices via the Active Directory group policy. You can install the Application Console the same way.

The protected devices on which you want to install Kaspersky Embedded Systems Security for Windows or the Application Console must be in the same domain and a single organizational unit.

The operating systems on the protected devices on which you want to install Kaspersky Embedded Systems Security for Windows using the policy must be of the same bitness (32-bit or 64-bit).

You must have domain administrator rights.

To install Kaspersky Embedded Systems Security for Windows, use the ess_x86.msi or ess_x64.msi installation package. To install the Application Console, use the esstools.msi installation package.

Detailed information about the use of Active Directory group policies is provided in the documentation supplied by Microsoft.

To install Kaspersky Embedded Systems Security for Windows or the Application Console:

1. Save ess_x64(or x86).msi to a shared folder on the domain controller.

2. Save the key file in the same public folder on the domain controller.

3. In the same shared folder on the domain controller, create an install_props.json file that contains the lines below. This signifies that you agree to the terms of the End User License Agreement and Privacy Policy.

```
{
"EULA": "1",
"PRIVACYPOLICY": "1"
}
```

4. On the domain controller create a new policy for the group that the protected devices belong to.

5. Using the **Group Policy Object Editor**, create a new installation package in the **Computer Configuration** node. Specify the path to the msi file for Kaspersky Embedded Systems Security for Windows (or Application Console) in UNC (Universal Naming Convention) format.

6. Select the Windows Installer's **Always install with elevated privileges** check box in both the **Computer Configuration** node and in the **User Configuration** node of the selected group.

7. Apply the changes using the `gpupdate / force` command.

Kaspersky Embedded Systems Security for Windows will be installed on the protected devices of the group after they have been restarted.

Actions to perform after Kaspersky Embedded Systems Security for Windows installation

After installing Kaspersky Embedded Systems Security for Windows on the protected devices, it is recommended that you immediately update the application databases and run a Critical Areas scan. You can perform these actions from the Application Console.

You can also configure administrator notifications about Kaspersky Embedded Systems Security for Windows events.

Uninstalling Kaspersky Embedded Systems Security for Windows via Active Directory group policies

Dump and trace files are not deleted on uninstalling Kaspersky Embedded Systems Security for Windows. You can manually delete dump and trace files from the folder specified during the configuration of dump and trace files writing.

If you used an Active Directory group policy to install Kaspersky Embedded Systems Security for Windows (or the Application Console) on the group of protected devices, you can use this policy to uninstall Kaspersky Embedded Systems Security for Windows (or the Application Console).

You can uninstall the application only with the default uninstallation parameters.

Detailed information about the use of Active Directory group policies is provided in the documentation supplied by Microsoft.

If application management is password protected, you cannot uninstall Kaspersky Embedded Systems Security for Windows using Active Directory group policies.

To uninstall Kaspersky Embedded Systems Security for Windows (or the Application Console):

1. On the domain controller, select the organizational unit from whose protected devices you want to uninstall Kaspersky Embedded Systems Security for Windows or the Application Console.

2. Select the policy created for the installation of Kaspersky Embedded Systems Security for Windows and in the **Group Policies Object Editor**, in the **Software installation** node (**Computer Configuration** > **Software**

Settings > **Software installation**) open the context menu of the Kaspersky Embedded Systems Security for Windows (or the Application Console) installation package and select the **All tasks** > **Remove** command.

3. Select the uninstallation method **Immediately uninstall the software from users and computers**.

4. Apply the changes using the `gpupdate /force` command.

Kaspersky Embedded Systems Security for Windows is removed from the protected devices after they are restarted and before logging in to Microsoft Windows.

Checking Kaspersky Embedded Systems Security for Windows functions. Using the EICAR test virus

This section describes the EICAR test virus and how to use the EICAR test virus to check the Real-Time File Protection and On-Demand Scan features of Kaspersky Embedded Systems Security for Windows.

About the EICAR test virus

This test virus is designed to verify the operation of anti-virus applications. It was developed by the European Institute for Computer Antivirus Research (EICAR).

The test virus is not a malicious object and does not contain executable code for your device, but most vendors' anti-virus applications identify it as a threat.

The file containing this test virus is called eicar.com. You can download it from the EICAR website.

Before saving the file in a folder on the device's hard drive, make sure that Real-Time File Protection is disabled on that drive.

The eicar.com file contains a line of text. When scanning the file Kaspersky Embedded Systems Security for Windows detects the test threat in this line of text, assigns the **Infected** status to the file, and deletes it. Information about the threat detected in the file will appear in the Application Console and in the task log.

You can use the eicar.com file to check how Kaspersky Embedded Systems Security for Windows disinfects the infected objects and how it detects probably infected objects. To do this, open the file using a text editor, add one of the prefixes listed in the table below to the beginning of the line of text in the file, and save the file with a new name, such as eicar_cure.com.

To make sure that Kaspersky Embedded Systems Security for Windows processes the eicar.com file with a prefix, in the **Objects protection** security settings section, set the **All objects** value for the Real-Time Computer Protection tasks and Default On-Demand Scan tasks of Kaspersky Embedded Systems Security for Windows.

Prefixes in EICAR files

Prefix	File status after the scan and Kaspersky Embedded Systems Security for Windows action
No prefix	**Kaspersky Embedded Systems Security for Windows assigns the Infected status to the object and deletes it.**

SUSP–	Kaspersky Embedded Systems Security for Windows assigns the **Probably infected** status to the object detected by the heuristic analyzer and deletes it since probably infected objects are not disinfected.
WARN–	Kaspersky Embedded Systems Security for Windows assigns the **Probably infected** status to the object (the object's code partly matches the code of a known threat) and deletes it since probably infected objects are not disinfected.
CURE–	Kaspersky Embedded Systems Security for Windows assigns the **Infected** status to the object and disinfects it. If disinfection is successful, the entire text in the file is replaced with the word "CURE".

Checking the Real-Time File Protection and On-Demand Scan features

After installing Kaspersky Embedded Systems Security for Windows, you can confirm that Kaspersky Embedded Systems Security for Windows detects objects containing malicious code. To do this, use the EICAR test virus.

To check the Real-Time File Protection feature:

1. Download the eicar.com file from the EICAR website. Save it in a shared folder on the local drive of any device on the network.

   Before you save the file to the folder, make sure that Real-Time File Protection is disabled for the folder.

2. If you want to check that network user notifications are working, make sure that the Microsoft Windows Messenger Service is enabled both on the protected device and on the device where you saved the eicar.com file.

3. Open the Application Console on the protected device.

4. Copy the saved eicar.com file to the local drive of the protected device using one of the following methods:

   - To test notifications through a Terminal Services window, copy the eicar.com file to the protected device after connecting to the protected device using the Remote Desktop Connection utility.

   - To test notifications through the Microsoft Windows Messenger Service, use the device's network places to copy the eicar.com file from the device where you saved it.

Real-Time File Protection is working correctly if the following conditions are met:

- The eicar.com file is deleted from the protected device.

- In the Application Console, the task log gets the *Critical* status. The log has a new line with information about a threat in the eicar.com file.

- The following Microsoft Windows Messenger Service message appears on the device from which you copied the file: `Kaspersky Embedded Systems Security for Windows blocked access to <path to file on the device>\eicar.com on computer <network name of the device> at <time that event occurred>. Reason: Threat detected. Virus: EICAR-Test-File. User name: <user name>. Computer name: <network name of the device from which you copied the file>.`

Make sure that the Microsoft Windows Messenger Service is running on the device from which you copied the eicar.com file.

To check the On-Demand Scan feature:

1. Download the eicar.com file from the EICAR website. Save it in a shared folder on the local drive of any device on the network.

   Before you save the file to the folder, make sure that Real-Time File Protection is disabled for the folder.

2. Open the Application Console and expand the **On-Demand Scan** node in the Application Console tree.
3. Select the **Critical Areas Scan** child node.
4. On the **Scan scope settings** tab, open the context menu on the **Network** node and select **Add network file**.
5. Enter the network path to the eicar.com file on the remote device in UNC (Universal Naming Convention) format.
6. Select the **Path to object** check box to include the added network path in the scan scope.
7. Run the Critical Areas Scan task.

The On-Demand Scan is working as it should if the following conditions are met:

- The eicar.com file is deleted from the device's hard drive.
- In the Application Console, the task log gets the *Critical* status. The Critical Areas Scan task log has a new line with information about a threat in the eicar.com file.

Application interface

You can control Kaspersky Embedded Systems Security for Windows using the following interfaces:

- Local Application Console.
- Kaspersky Security Center Administration Console.
- Kaspersky Security Center Web Console.
- Kaspersky Security Center Cloud Console.

Kaspersky Security Center Administration Console

Kaspersky Security Center lets you remotely install and uninstall, start and stop Kaspersky Embedded Systems Security for Windows, configure application settings, change the set of available application components, add keys, and start and stop tasks.

The application can be managed via Kaspersky Security Center using the Kaspersky Embedded Systems Security for Windows Administration Plug-in. See detailed information about the Kaspersky Security Center interface in the *Kaspersky Security Center Help*.

Kaspersky Security Center Web Console and Cloud Console

Kaspersky Security Center Web Console (hereinafter also referred to as Web Console) is a web application intended for centrally performing the main tasks to manage and maintain the security system of an organization's network. Web Console is a Kaspersky Security Center component that provides a user interface. For detailed information about Kaspersky Security Center Web Console, please refer to the *Kaspersky Security Center Help*.

Kaspersky Security Center Cloud Console (hereinafter also referred to as the Cloud Console) is a cloud-based solution for protecting and managing an organization's network. For detailed information about Kaspersky Security Center Cloud Console, please refer to the *Kaspersky Security Center Cloud Console Help*.

Web Console and Cloud Console let you do the following:

- Monitor the status of your organization's security system.
- Install Kaspersky applications on devices within your network.
- Manage installed applications.
- View reports on the security system status.

Application licensing

This section provides information about the main concepts related to licensing of the application.

About the End User License Agreement

The *End User License Agreement* is a binding agreement between you and AO Kaspersky Lab, stipulating the terms on which you may use the application.

Carefully review the terms of the End User License Agreement before you start using the application.

You can read the terms of the End User License Agreement and the Privacy Policy, that describes processing and transmission of data, in the following ways:

- During the installation of Kaspersky Embedded Systems Security for Windows Console.
- From the **Start** menu (**All programs** > **Kaspersky Embedded Systems Security for Windows** > **EULA and Privacy Policy**) after the installation.
- During the installation of Kaspersky Fraud Prevention Cloud.
- By reading the file license.txt document included in the distribution kit.
- On the Kaspersky web site (https://www.kaspersky.ru/business/eula).

By confirming that you agree with the End User License Agreement when installing the application, you signify your acceptance of the terms of the End User License Agreement. If you do not accept the terms of the End User License Agreement, you must abort application installation and must not use the application.

About the license

A *license* is a time-limited right to use the application, granted under the End User License Agreement.

A valid license entitles you to receive use of the application in accordance with the terms of the End User License Agreement as well as receive technical support when necessary.

The scope of service and the period of application use depend on the type of license used to activate the application.

You can activate the application in two ways:

- Using a key file, which grants you the usage under the commercial license
- Using an activation code to purchase a commercial license.

You can purchase a Kaspersky Embedded Systems Security for Windows standard license or Kaspersky Embedded Systems Security for Windows Compliance Edition extended license, which includes two additional system inspection components: File Integrity Monitor and Log Inspection.

When a commercial license expires, the application continues to run, but the following features become unavailable:

- Integrating with Kaspersky Security Network
- Kaspersky Embedded Systems Security for Windows database update.

If the license key is removed, the application will continue to run. If you remove a license, the application continues to run; the **On-Demand Scan** and **Real-Time File Protection** tasks remain available, but all other tasks and Kaspersky Embedded Systems Security for Windows database updates will be unavailable. The same happens if Kaspersky adds your license to the denylist.

To continue using all Kaspersky Embedded Systems Security for Windows features, you must renew your the license.

To ensure maximum protection of your device, we recommend that you renew the license before it expires.

Make sure that the expiration date for the additional key is later than for the active one

About license certificate

A *license certificate* is a document that you receive along with a key file or an activation code (if applicable).

A license certificate contains the following information about the current license:

- Order number
- Information about the user who has been granted the license
- Information about the application that can be activated under the license provided
- Limit of the number of licensing units (e.g., devices on which the application or individual software components can be used under the license provided)
- License validity start date
- License expiration date or license term
- License type

About the key

A *key* is a sequence of bits with which you can activate and subsequently use the application in accordance with the terms of the End User License Agreement. A key is generated by Kaspersky.

You can add a key to the application by using a key file. After you add a key to the application, the key is displayed in the application interface as a unique alphanumeric sequence.

Kaspersky can add a key to the denylist due to violations of the License Agreement. If your key is blocked, a different key must be added in order for the application to work.

A key may be an "active key" or an "additional key".

An *active key* is the key that the application currently uses to function. A key for a commercial or trial license may be added as the active key. The application can have no more than one active key.

An *additional key* is a key that confirms the right to use the application but is not currently in use. An additional key automatically becomes active when the license associated with the current active key expires. An additional key may be added only if there is an active key.

About the key file

A *key file* is a file with the .key extension, provided to you by Kaspersky. Key files are designed to add a key that activates the application.

You receive a key file via email after purchasing Kaspersky Embedded Systems Security for Windows or ordering the trial version of Kaspersky Embedded Systems Security for Windows.

You do not need to connect to Kaspersky activation servers in order to activate the application with a key file.

You can restore a key file if it has been accidentally deleted. You may need a key file to register with Kaspersky CompanyAccount.

To recover a key file, you should perform any of the following actions:

- Contact the license vendor.
- Obtain a key file from the Kaspersky website based on the available activation code.

About activation code

An *activation code* is a unique sequence of 20 letters and numbers. You have to enter an activation code in order to add a key for activating Kaspersky Embedded Systems Security for Windows. You receive the activation code at the email address that you provided when you bought Kaspersky Embedded Systems Security for Windows or ordered the trial version of Kaspersky Embedded Systems Security for Windows.

To activate the application with an activation code, you need Internet access in order to connect to Kaspersky activation servers.

If you have lost your activation code after installing the application, it can be recovered. You may need the activation code to register a Kaspersky CompanyAccount, for example. To recover your activation code, contact the Kaspersky Lab partner from whom you purchased the license.

About data provision

The License Agreement for Kaspersky Embedded Systems Security for Windows, specifically the section entitled "Terms of data processing", specifies the terms, liability, and procedure for sending and processing the data indicated in this Guide. Before accepting the License Agreement, carefully review its terms as well as all documents linked to by the License Agreement.

The data Kaspersky receives from you when you use the application is protected and processed in accordance with the Privacy Policy available at www.kaspersky.com/Products-and-Services-Privacy-Policy.

The terms of the License Agreement and Privacy Policy are available during installation of Kaspersky Embedded Systems Security for Windows as a part of distribution kit and from the **Start** menu (**All programs** > **Kaspersky Embedded Systems Security for Windows** > **EULA and Privacy Policy**) after the installation.

During the Kaspersky Embedded Systems Security for Windows uninstallation, all the data stored by Kaspersky Embedded Systems Security for Windows on the protected device is deleted.

By accepting the terms of the End User License Agreement, you agree to automatically send the following data to Kaspersky:

- To support the mechanism for receiving updates – information about the installed application and its activation: identifier of the application being installed and its full version, including build number, type, and license identifier, installation identifier, update task identifier.
- To use the ability to navigate to Knowledge Base articles when application errors occur (Redirector service) – information about the application and link type: the name, locale, and full version number of the application, type of redirecting link, and error identifier.
- To manage confirmations for data processing – information about the status of acceptance of license agreements and other documents, that stipulate data transferring terms: identifier and version of the License Agreement or other document, as a part of which the data processing terms are accepted or declined; an attribute, signifying the user's action (confirmation or recall of the terms acceptance); date and time of status changes of the data processing terms acceptance.

Local data processing

While executing the application's primary functions described in this Guide, Kaspersky Embedded Systems Security for Windows locally processes and stores a set of data on the protected device.

The table below contains information about local processing and storing by Kaspersky Embedded Systems Security for Windows of data contained in reports.

Processing and storing of data contained in reports

Functional area	Event registration
Type of use	Kaspersky Embedded Systems Security for Windows stores the data locally and sends the data to the Administration Server. The Administration Server database stores information about application events that occur on the managed protected devices.
Storage	• %ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Embedded Systems Security\<product version>\Reports • %SystemRoot%\System32\Winevt\Logs\Kaspersky Security.evtx • Administration Server's database
Security measures	Access-control list.
Storage period	Kaspersky Embedded Systems Security for Windows stores the data until the uninstallation of Kaspersky Embedded Systems Security for Windows.

	During the Kaspersky Embedded Systems Security for Windows uninstallation, all the data stored by Kaspersky Embedded Systems Security for Windows on the protected device is deleted.
Purpose	Providing primary functionality.

Kaspersky Embedded Systems Security for Windows does not delete events in the Windows Event Log including events that occur when uninstalling Kaspersky Embedded Systems Security for Windows.

In order to provide event registration functionality, Kaspersky Embedded Systems Security for Windows processes the following data locally:

- Names, checksums (MD5, SHA-256) and attributes of processed files and full paths to them on the scanned media.
- Actions taken on scanned files by Kaspersky Embedded Systems Security for Windows.
- User actions taken on scanned files on the protected device.
- Information about accounts of users performing any actions on the protected network or protected device.
- Device Instance Path values for devices added to the Device Control rules.
- Information about processes and scripts running on the system: checksums (MD5, SHA-256) and full paths to executable files, information about digital certificates.
- Windows Firewall settings.
- Windows Event Log entries.
- Names of user accounts taking actions on scanned files on the protected device.
- Instances of executable files being started, and the types, names, checksums, and attributes of these files.
- Information about network activity:
  - The IP addresses of blocked external devices.
  - Processed IP addresses.
- Information about the Windows USN Journal status.

The following table contains information about the service data processed by the Kaspersky Embedded Systems Security for Windows. The service data includes: program parameters, quarantined and backup files, information in the program's service databases, license data.

The table below contains information about local processing and storing by Kaspersky Embedded Systems Security for Windows of data about parameters specified by a user.

Processing and storing of data about parameters specified by a user

Functional area	All Kaspersky Embedded Systems Security for Windows functionality
Type of use	Kaspersky Embedded Systems Security for Windows stores the data locally and sends the data to the Administration Server. The data is stored in Administration Server database.

	The data processed by the application locally is not automatically sent to Kaspersky or other third-party systems.
Storage	• %ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Embedded Systems Security\<product version>\ • Administration Server's database
Security measures	Access-control list.
Processing period	Kaspersky Embedded Systems Security for Windows stores the data until the uninstallation of Kaspersky Embedded Systems Security for Windows. During the Kaspersky Embedded Systems Security for Windows uninstallation, all the data stored by Kaspersky Embedded Systems Security for Windows on the protected device is deleted. Kaspersky Embedded Systems Security for Windows does not delete the data about parameters exported into configuration file. Kaspersky Embedded Systems Security for Windows does not delete Quarantine objects and Backup objects if the **Export quarantine objects** and **Export Backup objects** check boxes are selected in the Setup Wizard.
Purpose	Providing primary functionality.

For the specified purposes, Kaspersky Embedded Systems Security for Windows processes the following data locally:

- Objects placed in Quarantine or Backup.
- Information about user accounts (usernames and passwords) under which Kaspersky Embedded Systems Security for Windows runs tasks.
- Kaspersky Embedded Systems Security for Windows password.
- IP addresses and identifiers of blocked logon sessions.
- Windows Firewall settings and Windows Firewall rules settings.
- Checksums (MD5, SHA-256) and paths to executable files added to the Application Launch Control task rules.
- Device Instance Path values for devices added to the Device Control rules.
- Information about files and folders included in scopes of Kaspersky Embedded Systems Security for Windows tasks.
- IP addresses included or excluded from the protection scope.
- Information about events in the Windows Event Log.
- Information about detections with the use of iSwift or iChecker technology.
- Checksums (MD5, SHA-256), full paths and masks specified in exclusions settings.
- Information about processes added to the Trusted Zone.
- Information about added license keys.

- Information about digital certificates.
- Files unpacked from an archive or other composite object during the scan.

Kaspersky Embedded Systems Security for Windows processes and stores data as part of the application's basic functionality, including to log application events and receive diagnostic data. Locally processed data is protected in accordance with the configured and applied application settings.

Kaspersky Embedded Systems Security for Windows lets you configure the level of protection for data processed locally (Managing access permissions for Kaspersky Embedded Systems Security for Windows functions, Event registration. Kaspersky Embedded Systems Security for Windows logs). You can change user privileges to access processed data, change data retention periods for such data, entirely or partially disable functionality that involves data logging, and change the path and attributes of the folder on the drive where data is logged.

The data processed by the application locally is not automatically sent to Kaspersky or other third-party systems.

By default, all data locally processed by the application during operation is removed after Kaspersky Embedded Systems Security for Windows is uninstalled from the protected device.

Files with diagnostic information (trace and dump files), application events in the Windows Event Log, and files with exported Kaspersky Embedded Systems Security for Windows settings are an exception. We recommend that you delete these files manually.

You can find the detailed information about working with files containing diagnostic data of the application in the corresponding sections of this Guide.

You can delete Windows Event Log files containing Kaspersky Embedded Systems Security for Windows application events using standard operating system tools.

Local data processing by means of the application auxiliary components

The Kaspersky Embedded Systems Security for Windows installation package comprises the application auxiliary components, which can be installed on your device even if Kaspersky Embedded Systems Security for Windows is not installed on it. Such auxiliary components are:

- The Application Console. This component is included as part of Kaspersky Embedded Systems Security for Windows Administration Tools and is a Microsoft Management Console snap-in.
- The Administration Plug-in. This component provides a full integration with Kaspersky Security Center application.

While performing the main functions of the application described in this Guide, the application auxiliary components locally process and store a set of data on the protected device where they are installed, even if they are installed separately from Kaspersky Embedded Systems Security for Windows.

The application components locally process and store the following data:

- The Application Console: the name of the protected device with Kaspersky Embedded Systems Security for Windows installed (IP address or domain name) to which the Application Console last connected remotely; display parameters configured in the Microsoft Management Console snap-in; data about the last folder in which the user selected objects via the Application Console (using a system dialog opened by clicking the **Browse** button). The Application Console trace files can also contain the following data: the name of the protected device with Kaspersky Embedded Systems Security for Windows installed to which the remote connection was established, the name of the user account under which the remote connection was established.

- The Administration Plug-in can process and temporarily store data processed by Kaspersky Embedded Systems Security for Windows; for example, configured settings of application tasks and components, settings of Kaspersky Security Center policies, data sent in network lists.

The table below contains information about local processing and storing by Kaspersky Embedded Systems Security for Windows of data written in dump and trace files.

Kaspersky Embedded Systems Security for Windows locally processes and stores the following data written in dump and trace files:

- Information about actions performed by Kaspersky Embedded Systems Security for Windows on the protected device.
- Information about objects processed by Kaspersky Embedded Systems Security for Windows.
- Information about activity on the protected device that is processed by Kaspersky Embedded Systems Security for Windows.
- Information about errors that occurred during the running of Kaspersky Embedded Systems Security for Windows.

The data processed by the auxiliary components is not automatically sent to Kaspersky or other third-party systems.

By default, all data locally processed by the application auxiliary components during the operation is deleted after removal of these components.

The exception is trace files of auxiliary application components. We recommend that you delete these files manually.

Data in trace and dump files

Kaspersky Embedded Systems Security for Windows can, in accordance with the settings, write debug information to trace files for the purposes of technical support during the operation of Kaspersky Embedded Systems Security for Windows.

Kaspersky Embedded Systems Security for Windows dump files are generated by the operating system during application crashes and are overwritten by the next crash.

Trace and dump files can include any personal data of a user or confidential data of your organization.

Do not use Kaspersky Embedded Systems Security for Windows on devices for which data submission is prohibited by the policy of your organization.

By default, Kaspersky Embedded Systems Security for Windows does not record debug information.

Trace and dump files are not automatically submitted beyond the host on which they were generated. The content of trace files can be viewed using standard text file viewers. Trace and dump files are kept indefinitely and are not deleted when uninstalling Kaspersky Embedded Systems Security for Windows.

Debug information can be useful for Technical Support.

No special mechanisms are provided for limiting access to trace and dump files. The administrator can configure this data to be written to a protected folder.

The path to the trace and dump file folder is not configured by default. To use the trace and dump folder, the administrator must specify it.

Data in trace and dump files can contain:

- Information about actions performed by Kaspersky Embedded Systems Security for Windows on the protected device.
- Information about objects processed by Kaspersky Endpoint Agent.
- Errors arising during the operation of Kaspersky Endpoint Agent.

Activating the application with a key file

You can activate Kaspersky Embedded Systems Security for Windows by applying a key file.

If an active key has already been added to Kaspersky Embedded Systems Security for Windows and you add another key as the active key, the new key replaces the previously added key. The previously added key is removed.

If an additional key has already been added to Kaspersky Embedded Systems Security for Windows and you add another key as an additional key, the new key replaces the previously added key. The previously added additional key is removed.

If an active key and an additional key have already been added to Kaspersky Embedded Systems Security for Windows and you add a new key as the active key, the new key replaces the previously added active key; the additional key is not removed.

To activate Kaspersky Embedded Systems Security for Windows using a key file:

1. In the Application Console tree, expand the **Licensing** node.
2. In the results pane of the **Licensing** node, click the **Add key** link.
3. In the window that opens, click the **Browse** button.
4. Select a key file with the .key extension.

   You can also add a key as an additional key. To add a key as an additional key, select the **Use as additional key** check box.

5. Click the **OK** button.

The selected key file will be applied. Information about the added key will be available on the **Licensing** node.

Activating the application with an activation code

To activate the application using an activation code, the protected device must be connected to the internet.

You can activate Kaspersky Embedded Systems Security for Windows by using an activation code.

When activating the application with this method, Kaspersky Embedded Systems Security for Windows sends data to the activation server to verify the entered code:

- If the activation code verification is successful, the application is activated.
- If the activation code verification fails, the corresponding notification is displayed. In this case, you must contact the software vendor from whom you purchased your Kaspersky Embedded Systems Security for Windows license.
- If the number of activations with the activation code is exceeded, the corresponding notification is displayed. The application activation procedure is interrupted, and the application prompts you to contact Technical Support.

You can activate Kaspersky Embedded Systems Security for Windows with an activation code using the Application Console, or by creating the Activation of the Application group task via the Administration Plug-in or via the Web Plug-in.

To activate Kaspersky Embedded Systems Security for Windows with an activation code using the Application Console:

1. In the Application Console tree, expand the **Licensing** node.
2. In the results pane of the **Licensing** node, click the **Add activation code** link.
3. In the window that opens, enter the activation code in the **Activation code** field.
   - If you want to use the activation code as an additional key, enable **Use as additional key** check box.
   - To view information about a license, click the **Show license information** button. The information will be displayed in the **License information** block.
4. Click the **OK** button.

   Kaspersky Embedded Systems Security for Windows sends information about the applied activation code to the activation server.

Viewing information about current license

Viewing licensing information

Information about the status of the current license is displayed in the details pane of the **Kaspersky Embedded Systems Security** node of the Application Console. A key can have the following statuses:

- **Checking the key status** – Kaspersky Embedded Systems Security for Windows is checking the applied key file or activation code and waiting for a response about the current key status.
- **License expiration date** – Kaspersky Embedded Systems Security for Windows has been activated until the specified date and time. The key status is highlighted in yellow in the following cases:
  - The license will expire in 14 days and no additional key has been applied.
  - The added key has been added to the denylist and is about to be blocked.

- **License has expired** – Kaspersky Embedded Systems Security for Windows is not activated because the license has expired. The status is highlighted in red.
- **End User License Agreement has been violated** – Kaspersky Embedded Systems Security for Windows is not activated because the terms of the End User License Agreement have been violated. The status is highlighted in red.
- **Key is in denylist** – The added key has been blocked and added to the denylist by Kaspersky, for example, if the key has been used by third parties to activate the application illegally. The status is highlighted in red.

Viewing information about current license

To view the information about the current license,

in the Application Console tree, expand the **Licensing** node.

General information about the current license is displayed in the details pane of the **Licensing** node (see the table below).

General information about the license in the Licensing node

Field	Description
Activation code	The activation code. This field is filled in if you activate the application using an activation code.
Activation status	Information about the activation status of the application. The **Activation status** column of the **Licensing** node's details pane can have the following statuses: • **Applied** – if you have activated the application using an activation code or key file. • **Activation** – if you have applied an activation code to activate the application, but the activation process has not been finalized yet. The status changes to **Applied** after activation of the application is complete and the contents of the node's details pane are refreshed. • **Activation error** – if application activation failed. You can view the cause of unsuccessful activation in the task log.
Key	The key used to activate the application.
License type	License type: commercial or trial.
Expiration date	Expiry date and time of the license associated with an active key.
Activation code status or key status	Activation code status or key status: *Active* or *Additional*.

To view the detailed information about license,

on the **Licensing** node, open the context menu on the line with license data that you want to expand and select **Properties**.

In the **Key properties** window, the **General** tab displays detailed information about the current license, and the **Advanced** tab displays information about the customer and the contact details of Kaspersky or the retailer from whom you purchased Kaspersky Embedded Systems Security for Windows (see the table below).

Detailed license information in the Properties: <Activation code status or key status> window

Field	Description
General tab	
Key	The key used to activate the application.
Key addition date	Date when the key was added to the application.
License type	License type: commercial or trial.
Days till expiration	Number of days remaining until the expiration of the license associated with the active key.
Expiration date	Expiry date and time of the license associated with an active key. If you activate the application under unlimited subscription, the field value is *Unlimited*. If Kaspersky Embedded Systems Security for Windows is unable to determine the license expiry date, the field value is set to *Unknown*.
Application	The name of the application activated with the key file or activation code.
Key usage restriction	Restriction on use of the key (if any).
Eligible for technical support	Information on whether Kaspersky or one of its partners will provide technical support under the license terms.
Advanced tab	
Information about the license	Current license key.
Support information	Contact details of Kaspersky or of its partner providing technical support. This field may be empty if technical support is not provided.
Owner information	Information about the license owner: a customer name and the name of the organization for which the license was acquired.

Functional limitations when the license expires

When the current license expires, the following limitations are applied to the functional components:

- All tasks are stopped, except the Real-Time File Protection, On-Demand Scan, Application Integrity Control and Network Threat Protection tasks.
- You cannot start any tasks except for Real-Time File Protection, On-Demand Scan, Application Integrity Control and Network Threat Protection tasks. These tasks continue to run using the old anti-virus databases.
- Exploit Prevention functionality is limited:

- Processes are protected until they are restarted.
- New processes cannot be added to the protection scope.

Other functions (repositories, logs, diagnostic information) are still available.

Renewing license

By default, Kaspersky Embedded Systems Security for Windows notifies you when the license has 14 days remaining before expiration. In this case, the **License expiration date** status is highlighted in yellow in the results pane of the **Kaspersky Embedded Systems Security for Windows** node.

You can renew the license before the expiration date using an additional key. This ensures that your device remains protected after expiration of the current license and before you activate the application with a new license.

To renew a license:

1. Obtain a new activation code or a key file.
2. In the Application Console tree, select the **Licensing** node.
3. Perform one of the following actions in the results pane of the **Licensing** node:
   - If you want to renew a license using a key file:
     a. Click the **Add key** link.
     b. In the window that opens, click the **Browse** button.
     c. Select a new key file with the .key extension.
     d. Select the **Use as additional key** check box.
   - If you want to renew a license using an activation code:
     a. Click the **Add activation code** link.
     b. Enter the purchased activation code in the window that opens.
     c. Select the **Use as additional key** check box.

   An Internet connection is required to apply an activation code.
4. Click the **OK** button.

The additional key will be added and automatically applied upon expiration of the current Kaspersky Embedded Systems Security for Windows license.

Deleting the key

You can remove the added key.

If an additional key has been added to Kaspersky Embedded Systems Security for Windows and you remove the active key, the additional key automatically becomes the active key.

If you delete an added key, you can restore it by re-applying the key file.

To remove a key that has been added:

1. In the Application Console tree, select the **Licensing** node.
2. In the results pane of the **Licensing** node in the table containing information on added keys, select the key that you want to remove.
3. In the context menu of the line containing information on the selected key, select **Remove**.
4. Click the **Yes** button in the confirmation window to confirm that you want to delete the key.

   The selected key will be removed.

Working with the Administration Plug-in

This section provides information about the Kaspersky Embedded Systems Security for Windows Administration Plug-in and describes how to manage the application installed on a protected device or on a group of protected devices.

Managing Kaspersky Embedded Systems Security for Windows from Kaspersky Security Center

You can centrally manage several protected devices that have Kaspersky Embedded Systems Security for Windows installed and are joined to the same administration group via the Kaspersky Embedded Systems Security for Windows Administration Plug-in. Kaspersky Security Center also lets you separately configure the settings of each protected device included in the administration group.

An administration group is created manually via Kaspersky Security Center. The group includes several devices with Kaspersky Embedded Systems Security for Windows installed for which you want to configure the same control and protection settings. For details on using administration groups, see *Kaspersky Security Center Help*.

Application settings for a single protected device are unavailable if the operation of Kaspersky Embedded Systems Security for Windows on the protected device is controlled by an active Kaspersky Security Center policy.

Kaspersky Embedded Systems Security for Windows can be managed from Kaspersky Security Center in the following ways:

- **Using Kaspersky Security Center policies**. Kaspersky Security Center policies can be used to remotely configure the same protection settings for a group of devices. Task settings specified in the active policy have priority over task settings configured locally in the Application Console or remotely in the **Properties: <Protected device name>** window of Kaspersky Security Center.

  Policies can be used to configure general application settings, settings for real-time computer protection tasks, activity control tasks on devices, and settings for starting local system tasks on a schedule.

- **Using Kaspersky Security Center group tasks**. Kaspersky Security Center group tasks allow remote configuration of common settings of tasks with an expiration period for a group of devices.

  You can use group tasks to activate the application, configure On-Demand Scan task settings, update task settings, and Rule Generator for Applications Launch Control task settings.

- **Using tasks for a set of devices**. Tasks for a set of devices allow remote configuration of common task settings with a limited execution period for protected devices that do not belong to any administration group.

- **Using the properties window of a single device**. In the **Properties: <Protected device name>** window, you can remotely configure the task settings for an individual protected device included in an administration group. You can also configure both general application settings and settings for all Kaspersky Embedded Systems Security for Windows tasks if the selected protected device is not controlled by an active Kaspersky Security Center policy.

Kaspersky Security Center allows you to configure application settings and advanced features, and also work with logs and notifications. You can configure these settings for a group of protected devices and for an individual protected device.

Managing application settings

This section contains information about configuring Kaspersky Embedded Systems Security for Windows general settings in Kaspersky Security Center Web Console.

Navigation

Learn how to navigate to the required task settings via the chosen interface.

Opening general settings via the policy

To open the application settings of the Kaspersky Embedded Systems Security for Windows via the policy:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure the task.
3. Select the **Policies** tab.
4. Double-click the policy name you want to configure.
5. In the **Properties: <Policy name>** window that opens, select the **Application settings** section.
6. Click the **Settings** button in the subsection of the setting that you want to configure.

Opening general settings in the application properties window

To open the properties window of the Kaspersky Embedded Systems Security for Windows for a single protected device:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure the task.
3. Select the **Devices** tab.
4. Open the **Properties: <Protected device name>** window in one of the following ways:
   - Double-click the name of the protected device.
   - Open the context menu of the protected device name and select the **Properties** item.

   The **Properties: <Protected device name>** window opens.
5. In the **Applications** section, select **Kaspersky Embedded Systems Security 3.4 for Windows**.

6. Click the **Properties** button.

   The **Kaspersky Embedded Systems Security 3.4 for Windows Settings** window opens.

7. Select the **Application settings** section.

Configuring general application settings in Kaspersky Security Center

You can configure Kaspersky Embedded Systems Security for Windows general settings from Kaspersky Security Center for a group of protected devices or for one protected device.

Configuring scalability, interface, and scan settings in Kaspersky Security Center

To configure scalability, interface, and scan settings:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of protected devices, select the **Policies** tab and open the **Properties: <Policy name>** window.
   - To configure the settings of a task or application for an individual protected device, select the **Devices** tab and go to local task settings or application settings.
4. In the **Application settings** section, in the **Scalability, interface and scan settings** subsection, click the **Settings** button.
5. In the **Advanced application settings** window on the **General** tab, configure the following settings:
   - In the **Scalability settings** section, configure the settings that define the number of processes used by Kaspersky Embedded Systems Security for Windows:
     - Automatically detect scalability settings
     - Set the number of working processes manually
       - Number of processes for real-time protection
       - Number of processes for background on-demand scan tasks
   - In the **Interaction with user** section, configure whether the System Tray Icon will be displayed in the notification area by clearing or selecting the **Display System Tray Icon in the taskbar** check box.
6. On the **Scan settings** tab, configure the following settings:
   - Restore file attributes after scanning

- Limit CPU usage for scanning threads
  - Upper limit (per cent)
- Folder for temporary files created during scanning

7. On the **Hierarchical storage** tab, select the option for accessing the hierarchical storage.
8. Click the **OK** button.

The configured application settings are saved.

Configuring security settings in Kaspersky Security Center

To configure security settings manually:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of protected devices, select the **Policies** tab and open the **Properties: <Policy name>** window.
   - To configure the settings of a task or application for an individual protected device, select the **Devices** tab and go to local task settings or application settings.
4. In the **Application settings** section, click the **Security and reliability** button in the **Settings** subsection.
5. In the **Security settings** window, configure the following settings:
   - In the **Password protection settings** section, enable or disable the **Protect application processes from external threats** option.
   - In the **Password protection settings** section, set a password to protect access to Kaspersky Embedded Systems Security for Windows functions.
   - In the **Self-defense** section, configure the settings for recovery of Kaspersky Embedded Systems Security for Windows tasks when the application returns an error or terminates.
     - Perform task recovery
     - Reliability settings
   - In the **Recover on-demand scan tasks no more than (times)** section, specify limitations on protected device load created by Kaspersky Embedded Systems Security for Windows after switching to UPS power:
     - Do not start scheduled scan tasks
     - Stop current scan tasks
   - In the **Password protection settings** section, set a password to protect access to Kaspersky Embedded Systems Security for Windows functions.

6. Click the **OK** button.

The scalability and reliability settings are saved.

Configuring connection settings using Kaspersky Security Center

The configured connection settings are used to connect Kaspersky Embedded Systems Security for Windows to update and activation servers and during integration of applications with KSN services.

To configure the connection settings take the following steps:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of protected devices, select the **Policies** tab and open the **Properties: <Policy name>** window.
   - To configure the settings of a task or application for an individual protected device, select the **Devices** tab and go to local task settings or application settings.
4. In the **Application settings** section, click the **Connections** button in the **Settings** subsection.

   The **Connection settings** window opens.
5. In the **Connection settings** window, configure the following settings:
   - In the **Proxy server settings** section, select the proxy server usage settings:
     - **Do not use proxy server**
     - Use the specified proxy server
     - **IP address or symbolic name of the proxy server and the port number**
     - **Do not use proxy server for local addresses**.
   - In the **Proxy server authentication settings** section, specify the authentication settings:
     - Select the authentication settings in the drop-down list.
       - **Do not use authentication** – authentication is not performed. The mode is selected by default.
       - **Use NTLM authentication** – authentication is performed using the NTLM network authentication protocol developed by Microsoft.
       - **Use NTLM authentication with user name and password** – authentication is performed with a user name and password using the NTLM network authentication protocol developed by Microsoft.
       - **Apply user name and password** – authentication is performed using the user name and password.
     - Enter the user name and password, if needed.

- In the **Licensing** section, clear or select the **Use Kaspersky Security Center as a proxy server when activating the application**.

6. Click the **OK** button.

The configured connection settings are saved.

Configuring scheduled start of local system tasks

You can use policies to allow or block start of the local system On-Demand Scan task and the Update task according to the schedule configured locally on each protected device in the administration group:

- If the scheduled start of a specific type of local system task is prohibited by a policy, these tasks will not be performed on the protected device according to the schedule. You can start local system tasks manually.
- If the scheduled start of a specific type of local system task is allowed by a policy, these tasks will be performed in accordance with the scheduled parameters configured locally for this task.

By default, starting a local system task is prohibited by policy.

We recommend that you do not allow local system tasks to start if updates or on-demand scans are administered by Kaspersky Security Center group tasks.

If you do not use group update or on-demand scan tasks, allow local system tasks to be started in the policy. Kaspersky Embedded Systems Security for Windows will perform application database and module updates, and start all local system on-demand scan tasks in accordance with the default schedule.

You can use policies to allow or block the scheduled start of the following local system tasks:

- On-Demand Scan tasks: Critical Areas Scan, Quarantine Scan, Scan at Operating System Startup, Application Integrity Control, Baseline File Integrity Monitor.
- Update tasks: Database Update, Software Modules Update, Copying Updates.

If the protected device is excluded from the administration group, the local system tasks schedule will be enabled automatically.

To allow or block the scheduled start of Kaspersky Embedded Systems Security for Windows local system tasks in a policy:

1. In the **Managed devices** node in the Administration Console tree, expand the required group and select the **Policies** tab.
2. On the **Policies** tab, in the context menu of the policy for which you want to schedule Kaspersky Embedded Systems Security for Windows local system tasks for the group of protected devices, select **Properties**.
3. In the **Properties: <Policy name>** window, open the **Application settings** section. In the **Run local system tasks** section, click the **Settings** button and do one of the following:
   - Select the **On-demand scan tasks** and **Update tasks and Copying Update task** check boxes to allow the scheduled launch of the listed tasks.

- Clear the **On-demand scan tasks** and **Update tasks and Copying Update task** check boxes to disable the scheduled launch of the listed tasks.

Selecting or clearing the check box will not affect the start settings of any local custom tasks of this type.

4. Make certain that the policy you are configuring is active and applied to the selected group of protected devices.

5. Click the **OK** button.

The configured task schedule settings are applied for the selected tasks.

Configuring Quarantine and Backup settings in Kaspersky Security Center

To configure general Backup settings in Kaspersky Security Center:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.

2. Select the administration group for which you want to configure application settings.

3. Perform one of the following actions in the details pane of the selected administration group:

   - To configure application settings for a group of protected devices, select the **Policies** tab and open the **Properties: <Policy name>** window.

   - To configure the settings of a task or application for an individual protected device, select the **Devices** tab and go to local task settings or application settings.

4. In the **Supplementary** section, click the **Settings** button in the **Storages** subsection.

5. Use the **Storages settings** tab of the **Backup** window to configure the following Backup settings:

   - If you want to specify the backup folder, use the **Backup folder** field to select the required folder on the local drive of the protected device, or enter its full path.

   - To set the maximum Backup size, select the **Maximum Backup size (MB)** check box and specify the relevant value in megabytes in the entry field.

   - To set the Backup free space threshold:

     - Define the value of the **Maximum Backup size (MB)** setting.

     - Select the **Threshold value for space available (MB)** check box.

     - Specify the minimum value of free space in the Backup folder in megabytes.

   - To specify a folder for restored objects, do one of the following:

     - Select the relevant folder on a local drive of the protected device in the **Restoration settings** section.

     - Enter the name of the folder and the full path to it in the **Target folder for restoring objects** field.

6. In the **Storages settings** window on the **Quarantine** tab, configure the following Quarantine settings:

- To change the Quarantine folder, in the **Quarantine folder** entry field specify the complete path to the folder on the local drive of the protected device.
- To set the maximum Quarantine size, select the **Maximum Quarantine size (MB)** check box and specify the value of this parameter in megabytes in the entry field.
- To set the minimum amount of free space in Quarantine, select the **Maximum Quarantine size (MB)** check box and the **Threshold value for space available (MB)** check box, and then specify the value of this parameter in megabytes in the entry field.
- To change the folder to which objects are restored from Quarantine, in the **Target folder for restoring objects** field specify the complete path to the folder on the local drive of the protected device.

7. Click the **OK** button.

The configured Quarantine and Backup settings are saved.

Creating and configuring policies

This section provides information on using Kaspersky Security Center policies for managing Kaspersky Embedded Systems Security for Windows on several protected devices.

Global Kaspersky Security Center policies can be created for managing protection on several devices where Kaspersky Embedded Systems Security for Windows is installed.

A policy enforces the specified Kaspersky Embedded Systems Security for Windows settings, functions and tasks on all protected devices for one administration group.

Several policies for one administration group can be created and enforced in turns. The policy currently active for a group has *active* status in the Administration Console.

Information on policy enforcement is logged in the Kaspersky Embedded Systems Security for Windows system audit log. This information can be viewed in the Application Console in the **System audit log** node.

Kaspersky Security Center offers one way to apply policies on protected devices: *Prohibit changing the settings*. After a policy has been applied, Kaspersky Embedded Systems Security for Windows uses the values of settings for which you have selected the icon in the policy properties on protected devices. In this case, Kaspersky Embedded Systems Security for Windows does not use the values of settings in effect before the policy was applied. Kaspersky Embedded Systems Security for Windows does not apply the values of active policy settings for which the icon is selected in the policy properties.

If a policy is active, the values of settings marked with the icon in the policy are displayed in the Application Console but cannot be edited. The values of other settings (marked with the icon in the policy) can be edited in the Application Console.

The settings configured in the active policy and marked with the icon also block changes in Kaspersky Security Center for one protected device in the **Properties: <Protected device name>** window.

Settings that are specified and sent to the protected device using an active policy are saved in the local task settings after the active policy is disabled.

If a policy defines the settings of a currently running Real-Time Computer Protection task, the settings defined by the policy will change immediately after the policy is applied. If the task is not running, the settings are applied when it starts.

Creating a policy

To create a policy for a group of protected devices where application is installed and running:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree, then select the administration group containing the protected devices for which you wish to create a policy.
2. In the details pane of the selected administration group, select the **Policies** tab and click the **Create a policy** link to start the wizard and create a policy.

   The **New Policy Wizard** window opens.
3. In the **Select the application for which you want to create a group policy** window, select Kaspersky Embedded Systems Security for Windows and click **Next**.
4. Enter a group policy name in the **Name** field.

   The policy name cannot contain the following symbols: `" * < : > ? \ |` .
5. To apply a policy configuration used in a previous version of the application:

   a. Select the **Use settings from policy for previous versions of application** check box.

   b. Click the **Browse** button.

   c. Select the policy you want to apply.

   d. Click the **Next** button.
6. In the **Operation type selection** window, in the **Policy creation method** block, select one of the following options:

   - **New**, to create a new policy with default settings.
   - **Import policy created with previous versions of Kaspersky Embedded Systems Security for Windows**, to use the imported policy as a template.
7. In the **Real-Time Computer Protection** window, configure the application components:

   a. If necessary, change the default settings of the Real-Time Computer Protection components:

      1. Click **Settings** in the component subsection.
      2. In the window that opens, configure the component settings:
      3. Click the **OK** button.

   b. Allow or block the application of the settings of Real-Time Computer Protection components on protected devices in the network:

      - Click the button to allow configuration of the application component settings on protected devices in the network and to block the application of the application component settings configured in the policy.

- Click the button to block the configuration of the application component settings on protected devices in the network and to allow the application component settings configured in the policy to be applied.

c. Click the **Next** button.

8. Select one of the following policy statuses in the **Create the group policy for the application** window:

- **Active policy**, if you want to apply the policy immediately after it is created. If an active policy already exists in the group, it is deactivated and a new policy is applied.
- **Inactive policy** if you do not want to apply the created policy immediately. In this case the policy may be activated later.
- Select the **Open policy properties immediately after they are created** check box to automatically close the **New Policy Wizard** and configure the newly created policy after clicking the **Next** button.

9. Click the **Finish** button.

The created policy appears in the list of policies on the **Policies** tab of the selected administration group. In the **Properties: <Policy name>** window, you can configure other settings, tasks and functions of Kaspersky Embedded Systems Security for Windows.

After a new policy is created, a set of allowing rules is created to prevent applications from being blocked, ensuring their uninterrupted operation. You can view the default rules in the task settings. See below for details and limitations.

By default, Kaspersky Embedded Systems Security for Windows creates a set of rules for inbound network traffic when creating a new policy:

- Two allowing rules for the process of sharing the Windows desktop using Kaspersky Security Center Network Agent, which is located in the %Program Files% and %Program Files (x86)% folders. Status: enabled. Allowed external addresses: all. Protocols: TCP and UDP, one rule per protocol.
- Two allowing rules for local port 15000. State: enabled. Allowed external addresses: all. Protocols: TCP and UDP, one rule per protocol.

By default, Kaspersky Embedded Systems Security for Windows creates a set of outgoing network traffic rules when creating a new policy:

- Two allowing rules for the Kaspersky Embedded Systems Security for Windows service, which is located in the %Program Files% and %Program Files (x86)% folders. Status: enabled. Allowed external addresses: all. Protocols: TCP and UDP, one rule per protocol.
- Two allowing rules for the worker process of Kaspersky Embedded Systems Security for Windows, which is located in the %Program Files% and %Program Files (x86)% folders. Status: enabled. Allowed external addresses: all. Protocols: TCP and UDP, one rule per protocol.
- Two allowing rules for local port 13000. State: enabled. Allowed external addresses: all. Protocols: TCP and UDP, one rule per protocol.

Kaspersky Embedded Systems Security for Windows policy settings sections

General

In the **General** section, you can configure the following policy settings:

- Indicate the policy status.
- Configure the inheritance settings for parent and child policies.

Event notification

In the **Event notification** section, you can configure settings for the following event categories:

- *Critical event*
- *Functional failure*
- *Warning*
- *Info*
  You can use the **Properties** button to configure the following settings for the selected events:
- Indicate the storage location and retention period for information about logged events.
- Indicate the notification method for logged events.

Application settings

Settings of the Application Settings section

Section	Options
Scalability, interface and scan settings	In the **Scalability, interface and scan settings** subsection, you can click the **Settings** button to configure the following settings: • Choose whether to configure scalability settings automatically or manually. • Configure the application icon display settings.
Security and reliability	In the **Security and reliability** subsection, you can click the **Settings** button to configure the following settings: • Configure the task start settings. • Specify how the application should behave when the protected device is running on UPS power. • Enable or disable password-protection of application functions.
Connections	In the **Connections** subsection, you can use the **Settings** button to configure the

	following proxy server settings for connecting with update servers, activation servers, and KSN: • Configure the proxy server settings. • Specify the proxy server authentication settings.
Run local system tasks	In the **Run local system tasks** subsection, you can use the **Settings** button to allow or block the start of the following local system tasks according to a schedule configured on protected devices: • On-Demand Scan task. • Update tasks and Copying Update task.

Supplementary

Settings of the Supplementary section

Section	Options
Trusted Zone	In the **Settings** subsection, you can click the **Trusted Zone** button to configure the following Trusted Zone settings: • Create a list of Trusted Zone exclusions. • Enable or disable scanning of file backup operations. • Create a list of trusted processes.
Removable Drives Scan	In the **Removable Drives Scan** subsection, you can use the **Settings** button to configure scan settings for removable drives.
User access permissions for application management	In the **User access permissions for application management** subsection, you can configure user rights and user group rights to manage Kaspersky Embedded Systems Security for Windows.
User access permissions for Kaspersky Security Service management	In the **User access permissions for Kaspersky Security Service management** subsection, you can configure user rights and user group rights to manage the Kaspersky Security Service.
Storages	In the **Storages** subsection, click the **Settings** button to configure the following Quarantine, Backup and Blocked Hosts settings: • Specify the path to the folder where you want to place Quarantine or Backup objects. • Configure the maximum size of Backup and Quarantine and also specify the available space threshold. • Specify the path to the folder where you want to place objects restored from Quarantine or Backup. • Configure how long hosts are blocked.

Real-Time Computer Protection

Settings of the Real-Time Computer Protection section

Section	Options
Real-Time File Protection	In the **Real-Time File Protection** subsection, you can click the **Settings** button to configure the following settings: • Indicate the protection mode. • Configure use of the Heuristic Analyzer. • Configure application of the trusted zone. • Indicate the protection scope. • Set the security level for the selected protection scope: you can select a predefined security level or configure the security settings manually. • Configure the task start settings.
KSN Usage	In the **KSN Usage** subsection, you can click the **Settings** button to configure the following task settings: • Indicate the actions to perform on KSN untrusted objects. • Configure data transfer and usage of Kaspersky Security Center as a KSN proxy server. Click the **KSN Statement** button to accept or reject the KSN Statement, and configure data exchange settings.
Exploit Prevention	In the **Exploit Prevention** subsection, you can click the **Settings** button to configure the following task settings: • Select the process memory protection mode. • Indicate actions to reduce exploit risks. • Add to and edit the list of protected processes.

Local activity control

Settings of the Local Activity Control section

Section	Options
Applications Launch Control	In the **Applications Launch Control** subsection, you can use the **Settings** button to configure the following task settings: • Select the task operating mode. • Configure settings for controlling subsequent application launches. • Indicate the scope of the Applications Launch Control rules. • Configure use of KSN. • Configure the task start settings.

Device Control	In the **Device Control** subsection, you can click the **Settings** button to configure the following task settings: • Select the task operating mode. • Configure the task start settings.

Network activity control

Settings of the Network activity control section

Section	Options
Firewall Management	In the **Firewall Management** subsection, you can click the **Settings** button to configure the following task settings: • Configure firewall rules. • Configure the task start settings.

System inspection

Settings of the System Inspection section

Section	Options
File Integrity Monitor	In the **File Integrity Monitor** subsection, you can configure control over changes in files that can signify a security breach on a protected device.
Log Inspection	In the **Log Inspection** subsection, you can configure monitoring of the integrity of the protected device based on the results of an analysis of the Windows Event Log.

Logs and notifications

Settings of the Logs and Notifications section

Section	Options
Task logs	In the **Task logs** subsection, you can click the **Settings** button to configure the following settings: • Specify the importance level of the logged events for the selected software components. • Specify the task log storage settings. • Specify the SIEM integration with Kaspersky Security Center settings.
Event notifications	In the **Event notifications** subsection, you can click the **Settings** button to configure the following settings: • Specify the user notification settings for the *Object detected*, *Untrusted external device detected and restricted*, and *Network session listed as untrusted* events.

	• Specify the administrator notification settings for any event selected in the event list in the **Notification settings** section.
Interaction with Administration Server	In the **Interaction with Administration Server** section, you can click the **Settings** button to select the types of objects (including Quarantine and Backup objects) that Kaspersky Embedded Systems Security for Windows will report to Administration Server.

Crash diagnostics

Settings of the Malfunction diagnosis section

Section	Options
Crash diagnostics settings	In the **Troubleshooting settings** subsection, you can configure the following options: • Select the option to **Enable tracing**. • Define the **Folder for trace files**. • Specify the **Level of details**. • Define the **Maximum size of the trace files**. • Select the option to **Remove the oldest trace files**. • Define the **Maximum number of files for one trace log**. Group policy settings and local settings introduce matching parameters. For details on settings and their limitations, please see the description of how to configure local settings. You can set different values for the settings on the local device and in the group policy for multiple devices, with the following conditions applied: • Group policy settings configured on Kaspersky Security Center server are of higher priority over the local settings. • Group policy settings configured on the local device are of lower priority over the local settings.
Dump file settings	In the **Dump file settings** subsection, you can configure the following options as applicable: • Select the option to **Create the dump file**. • Define the **Dump file folder**. Group policy settings and local settings introduce matching parameters. For details on settings and their limitations, please see the description of how to configure local settings. You can set different values for the settings on the local device and in the group policy for multiple devices, with the following conditions applied: • Group policy settings configured on Kaspersky Security Center server are of higher priority over the local settings. • Group policy settings configured on the local device are of lower priority over the local settings.

Revision history

In the **Revision history** section, you can manage revisions: compare with the current revision or other policy, add descriptions of revisions, save revisions to a file or perform a rollback.

Configuring a policy

To configure the policy settings:

1. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node.
2. Expand the administration group for which you want to configure the associated policy settings, and open the **Policies** tab in the details pane.
3. Click the policy name you want to configure.
4. Open the **Properties: <Policy name>** window in one of the following ways:
   - Selecting the **Properties** option in the policy context menu.
   - Clicking the **Configure policy** link in the right details pane of the selected policy.
   - Double-clicking the selected policy.
5. On the **General** tab in the **Policy status** section, enable or disable the policy. To do so, select one of the options below:
   - **Active policy**, if you want the policy to be applied on all protected devices within the selected administration group.
   - **Inactive policy**, if you want to activate the policy later on all protected devices within the selected administration group.

   The **Out-of-office policy** setting is not available when you manage Kaspersky Embedded Systems Security for Windows.
6. Reconfigure the application in other sections of the policy.

   You can enable or disable the execution of any task on all protected devices within the administration group by means of a Kaspersky Security Center policy.

   You can configure the application of policy settings on all network protected devices for each individual software component.
7. Click the **OK** button.

The configured settings are applied in the policy.

Creating and configuring tasks using Kaspersky Security Center

This section contains information about Kaspersky Embedded Systems Security for Windows tasks, and how to create them, configure task settings, and start and stop them.

About task creation in Kaspersky Security Center

You can create group tasks for administration groups and sets of protected devices. You can create the following types of tasks via Kaspersky Security Center:

- Activation of Application
- Copying Updates
- Database Update
- Software Modules Update
- Rollback of Database Update
- On-Demand Scan
- Application Integrity Control
- Baseline File Integrity Monitor
- Rule Generator for Applications Launch Control
- Rule Generator for Device Control

You can create local and group tasks in the following ways:

- For one protected device: in the **Properties <Protected device name>** window in the **Tasks** section.
- For an administration group: in the details pane of the node of the selected group of protected devices on the **Tasks** tab.
- For a set of protected devices: in the details pane of the **Device selections** node.

You can use policies to disable schedules for update and On-Demand Scan local system tasks on all protected devices in the same administration group.

General information on tasks in Kaspersky Security Center is provided in the *Kaspersky Security Center Help*.

Creating a task using Kaspersky Security Center

To create a new task in the Kaspersky Security Center Administration Console:

1. Start the task wizard in one of the following ways:

   - To create a local task:

     a. Expand the **Managed devices** node in the Administration Console tree and select the group that the protected server belongs to.

     b. In the results pane of the **Devices** tab, open the context menu of the protected device and select **Properties**.

     c. In the window that opens, click the **Add** button in the **Tasks** section.

   - To create a group task:

     a. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.

     b. Select the administration group for which you want to create a task.

     c. In the results pane, open the **Tasks** tab and select **Create a task**.

   - To create a task for a custom set of protected devices:

     a. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.

     b. Select the administration group containing the protected devices.

     c. Select a protected device or a custom set of protected devices.

     d. From the **Perform action** drop-down list, select the **Create a task** option.

   The task wizard window opens.

2. In the **Select the task type** window, under the heading **Kaspersky Embedded Systems Security 3.4 for Windows**, select the type of the task to be created.

3. If you selected any task type except Rollback of Database Update, Application Integrity Control or Activation of the Application, the **Settings** window opens. Depending on the task type, the settings may vary:

   - Create an On-Demand Scan task.

   - To create an update task, configure task settings based on your requirements:

     a. Select an update source in the **Update source** window.

     b. Click the **Connection settings** button. In the **Connection settings** window, configure proxy server access settings when connecting to the update source.

   - To create a Software Modules Update task, configure the required application module update settings in the **Settings** window:

     a. Select whether to copy and install critical software module updates, or only to check for their availability without installation.

     b. If **Copy and install critical software modules updates** is selected: a protected device restart may be required to apply the installed software modules. If you wish Kaspersky Embedded Systems Security for

Windows to restart the protected device automatically upon task completion, select the **Allow operating system restart** check box.

c. To obtain information about Kaspersky Embedded Systems Security for Windows module upgrades, select **Receive information about available scheduled software modules updates**.

Kaspersky does not publish planned update packages on the update servers for automatic installation; these can be downloaded manually from the Kaspersky website. An administrator notification about the **New scheduled software modules update is available** event can be configured. This will contain the URL of our website from which scheduled updates can be downloaded.

- To create the Copying Updates task, specify the set of updates and the destination folder in the **Copying updates settings** window.
- To create the Activation of the Application task:

  a. In the **Activation Settings** window, specify the key file that you want to use to activate the application.

  b. Select the **Use as additional key** check box if you want to create a task for renewing the license.
- Create the Rule Generator for Applications Launch Control task.
- Create the Rule Generator for Device Control task.

4. Configure the task schedule.

   You can configure a schedule for all task types except the Rollback of Database Update task.
5. Click the **OK** button.
6. If the task is being created for a set of protected devices, select the network (or group) of protected devices on which this task will be executed.
7. In the **Selecting an account to run the task** window, specify the account you want to use to run the task.
8. In the **Define the task name** window, enter the task name (no longer than 100 characters) not containing the symbols " * < > ? \ | : .

   We recommend that you add the task type to the task name (for example, "On-demand scan of shared folders").
9. In the **Finishing creating the task** window:

   a. Select the **Run task after Wizard finishes** check box if you want the task to start as soon as it is created.

   b. Click the **Finish** button.

The task created is displayed in the **Tasks** list.

Going to the local task settings and general application settings for an individual computer

If the application is currently under the Kaspersky Security Center policy and this policy prohibits changing the application settings, you cannot edit these settings for an individual computer.

To go to the local task settings for an individual computer:

1. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node.
2. Select the group that the protected device belongs to.
3. In the results pane, select the **Devices tab**.
4. Open the **Properties: <Protected device name>** window in one of the following ways:
   - Double-click the name of the protected device.
   - in the context menu of the name of the protected device, select **Properties**.

   The **Properties: <Protected device name>** window opens.
5. Go to the **Tasks** section.
6. In the task list, select a local task to configure in one of the following ways:
   - double-click on the task name
   - select a task in the list and click the **Properties** button
   - in the context menu on the task name, select **Properties**.

   The **Properties: <Task name>** window opens.

To go to the general application settings for an individual computer:

1. Expand the **Managed devices** node in the tree of the Administration Server of Kaspersky Security Center and select the group that the protected device belongs to.
2. In the results pane, select the **Devices** tab.
3. Open the **Properties: <Protected device name>** window in one of the following ways:
   - Double-click the name of the protected device.
   - in the context menu of the name of the protected device, select **Properties**.

   The **Properties: <Protected device name>** window opens.
4. Go to the **Applications** section.
5. In the list of installed applications, select Kaspersky Embedded Systems Security for Windows in one of the following ways:
   - double-click the name of Kaspersky Embedded Systems Security for Windows
   - select Kaspersky Embedded Systems Security for Windows in the list and click the **Properties** button.
   - in the context menu of the name of Kaspersky Embedded Systems Security for Windows, select the **Properties** item.

   The **Settings** window of **Kaspersky Embedded Systems Security for Windows** opens.

Configuring group tasks in Kaspersky Security Center

When managing Kaspersky Embedded Systems Security for Windows from Kaspersky Security Center Cloud Console, you cannot add custom HTTP and FTP servers or network folders manually.

To configure a group task for multiple protected devices:

1. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node and select the administration group for which you want to configure the application tasks.
2. In the details pane of a selected administration group, open the **Tasks** tab.
3. In the list of previously created group tasks, select a task you want to configure.
4. Open the **Properties: <Task name>** window in one of the following ways:
   - Double-click the name of the task in the list of created tasks.
   - Select the name of the task in the list of created tasks and click the **Configure task** link.
   - Open the context menu of the task name in the list of created tasks and select the **Properties** item.

   In the **Notification** section, configure the task event notification settings. For detailed information on configuring settings in this section, see *Kaspersky Security Center Help*.
5. Depending on the type of configured task, do one of the following:
   - To configure an On-Demand Scan task:
     - In the **Scan scope** section, configure a scan scope.
     - In the **Options** section, configure the task priority level and integration with other software components.
   - To configure an update task, adjust the task settings based on your requirements:
     - In the **Settings** section, configure update source settings and disk subsystem optimization.
     - Click the **Connection settings** button to configure update source connection settings.
   - To configure the Software Modules Update task:
     - Go to the **Settings** section.
     - Choose an action to perform: copy and install critical updates of software modules or only check for them.
   - To configure the Copying Updates task, specify the set of updates and the destination folder in the **Copying updates settings** section.
   - To configure an Activation of the Application task:

- In the **Activation Settings** section, specify the key file that you want to use to activate the application.
- Select the **Use as additional key** check box if you want to add an activation code or key file for renewing the license.

- To configure the automatic generation of allowing rules for Device Control, in the **Settings** section, specify the settings that will be used to create the list of allowing rules.

6. Configure the task schedule in the **Schedule** section. You can configure a schedule for all task types except the Rollback of Database Update task.

7. In the **Account** section, specify the account whose rights will be used to run the task. For detailed information on configuring settings in this section, see *Kaspersky Security Center Help*.

8. If required, specify the objects to exclude from the task scope in the **Exclusions from task scope** section. For detailed information on configuring settings in this section, see *Kaspersky Security Center Help*.

9. Click the **OK** button in the **Properties: <Task name>** window.

The newly configured group task settings are saved.

Configurable group task settings are summarized in the table below.

Kaspersky Embedded Systems Security for Windows group tasks settings

Kaspersky Embedded Systems Security for Windows task types	Section in the Properties: <Task name> window	Task settings
Rule Generator for Applications Launch Control	**Settings**	While configuring the Rule Generator for Applications Launch Control task settings you can select how to create allowing rules: • **Create allowing rules based on running applications** • **Create allowing rules for applications from the folders**
	Options	You can specify actions to perform while creating allowing rules for applications launch control: • **Use digital certificate** • **Use digital certificate subject and thumbprint** • **If the certificate is missing, use** • **Use SHA256 hash** • **Generate rules for user or group of users** You can configure settings for configuration files with allowing rule lists that Kaspersky Embedded Systems Security for Windows creates upon task completion.
	Schedule	You can configure settings to start the task on a schedule.
Rule Generator	**Settings**	• Select the operation mode: consider system data about all external

for Device Control		devices that have ever been connected or consider currently connected external devices only. • Configure settings for configuration files with allowing rule lists that Kaspersky Embedded Systems Security for Windows creates upon task completion.
	Schedule	You can configure settings to start the task on a schedule.
Activation of Application	**Activation Settings**	To activate the application or to renew the license, you can add a key file.
	Schedule	You can configure settings to start the task on a schedule.
Copying Updates	**Update source**	You can specify Kaspersky Security Center Administration Server or Kaspersky update servers as an application update source. You can also create a customized list of update sources: by adding custom HTTP and FTP servers or network folders manually and setting them as update sources. You can specify the usage of Kaspersky update servers, if manually customized servers are not available.
	Connection settings window	In the **Connection settings** window linked from the **Update source** section, you can specify whether a proxy server should be used to establish the connection to Kaspersky update servers or any other server.
	Copying updates settings	You can specify the set of updates intended for copying. In the **Folder for local storage of copied updates** field, specify a path to the folder that will be used by Kaspersky Embedded Systems Security for Windows to store copied updates.
	Schedule	You can configure settings to start the task on a schedule.
Database Update	**Settings**	You can specify Kaspersky Security Center Administration Server or Kaspersky update servers as an application update source in the **Update source** group box. You can also create a customized list of update sources: by adding custom HTTP and FTP servers or network folders manually and setting them as update sources. You can specify the usage of Kaspersky update servers, if manually customized servers are not available. In the Disk I/O usage optimization section you can configure the feature that reduces the workload on the disk subsystem: • **Lower the load on the disk I/O** • **RAM used for optimization (MB)**
	Connection settings window	In the **Connection settings** window linked from the **Update source** section, you can specify whether a proxy server should be used to establish the connection to Kaspersky update servers or any other server.
	Schedule	You can configure settings to start the task on a schedule.
Software Modules Update	**Update source**	You can specify Kaspersky Security Center Administration Server or Kaspersky update servers as an application update source. You can also create a customized list of update sources: by adding custom HTTP and FTP servers or network folders manually and setting them as update sources. You can specify the usage of Kaspersky update servers, if manually customized servers are not available.

	Connection settings window	In the **Update source connection settings** group box, you can specify whether a proxy server should be used to establish the connection to Kaspersky update servers or any other server.
	Settings	You can specify the actions that Kaspersky Embedded Systems Security for Windows will perform if critical application module updates are needed, as well as after installation of critical updates is complete. In addition, you can specify whether Kaspersky Embedded Systems Security for Windows will receive information about available scheduled updates.
	Schedule	You can configure settings to start the task on a schedule.
On-Demand Scan Settings	**Scan scope**	You can specify a scan scope for the On-Demand Scan task and configure security level settings.
	On-demand scan settings window	In the **On-demand scan settings** window linked from the **Scan scope** section, you can select one of the predefined security levels or customize a security level manually.
	Options	In the **Heuristic analyzer** settings block, you can enable or disable use of the heuristic analyzer for the On-Demand Scan task and set the analysis level using a slider. In the **Integration with other components** group box, you can configure the following settings: • Apply Trusted Zone for On-Demand Scan tasks. • Apply KSN usage for On-Demand Scan tasks. • Set a priority for the On-Demand Scan task: perform task in background mode (low priority) or consider task a Critical Areas Scan.
	Schedule	You can configure settings to start the task on a schedule.
Application Integrity Control	**Schedule**	You can configure settings to start the task on a schedule.
Baseline File Integrity Monitor	**Schedule**	You can configure settings to start the task on a schedule.

For the Rollback of Database Update task, you can configure only the standard task settings controlled by Kaspersky Security Center in the **Notification** and **Exclusions from task scope** sections.

For detailed information on configuring settings in these sections, see *Kaspersky Security Center Help*.

Activation of the Application task

To configure an Activation of the Application task:

1. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node and select the administration group for which you want to configure the application tasks.

2. In the details pane of a selected administration group, open the **Tasks** tab.
3. In the list of previously created group tasks, select a task you want to configure.
4. Open the **Properties: <Task name>** window in one of the following ways:
   - Double-click the name of the task in the list of created tasks.
   - Select the name of the task in the list of created tasks and click the **Configure task** link.
   - Open the context menu of the task name in the list of created tasks and select the **Properties** item.

   In the **Notification** section, configure the task event notification settings. For detailed information on configuring settings in this section, see *Kaspersky Security Center Help*.
5. In the **Activation Settings** section, specify the key file that you want to use to activate the application. Select the **Use as additional key** check box if you want to add a key to renew the license.
6. Configure the task schedule in the **Schedule** section (you can configure a schedule for all task types except Rollback of Database Update).
7. In the **Account** section, specify the account whose rights will be used to run the task.
8. If required, specify the objects to exclude from the task scope in the **Exclusions from task scope** section.

   For detailed information on configuring settings in these sections, see *Kaspersky Security Center Help*.
9. Click the **OK** button in the **Properties: <Task name>** window.

   The newly configured group task settings are saved.

Update tasks

To configure the Copying Updates, Database Update, or Software Modules Update tasks:

1. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node and select the administration group for which you want to configure the application tasks.
2. In the details pane of a selected administration group, open the **Tasks** tab.
3. In the list of previously created group tasks, select a task you want to configure.
4. Open the **Properties: <Task name>** window in one of the following ways:
   - Double-click the name of the task in the list of created tasks.
   - Select the name of the task in the list of created tasks and click the **Configure task** link.
   - Open the context menu of the task name in the list of created tasks and select the **Properties** item.

In the **Notification** section, configure the task event notification settings. For detailed information on configuring settings in this section, see *Kaspersky Security Center Help*.

5. In the **Update source** section, do the following:

   a. Select the update source:

   - Kaspersky Security Center Administration Server.
   - Kaspersky update servers.
   - Custom HTTP or FTP servers, or network folders.

   To use an SMB-shared folder as an update source, you need to specify a user account to start a task.

   You can specify the usage of Kaspersky update servers, if manually customized servers are not available.

   b. Click the **Connection settings** button.

   c. In the **Connection settings** window that opens, configure the use of a proxy server for connecting to Kaspersky update servers and other servers.

   d. For the Database Update task, in the **Disk I/O usage optimization** section, configure the feature that reduces the workload on the disk subsystem:

   The **Disk I/O usage optimization** section is available only for the Database Update task.

   - **Lower the load on the disk I/O**
   - **RAM used for optimization (MB)**

6. For the Software Modules Update task, in the **Settings** section, specify which actions Kaspersky Embedded Systems Security for Windows should perform when critical software module updates are available or information about planned updates is available.

   You can also specify which actions Kaspersky Embedded Systems Security for Windows should perform when critical updates are installed.

   The **Settings** section is available only for the Software Modules Update task.

7. For the Copying Updates task, in the **Copying updates settings** section, specify the set of updates and the destination folder.

   The **Copying updates settings** section is available only for the Copying Updates task.

8. Configure the task schedule in the **Schedule** section (you can configure a schedule for all task types except Rollback of Database Update).

9. In the **Account** section, specify the account whose rights will be used to run the task.

For detailed information on configuring settings in these sections, see *Kaspersky Security Center Help*.

10. In the **Properties: <Task name>** window, click **OK**.

The newly configured group task settings are saved.

For the Rollback of Database Update task, you can configure only the standard task settings controlled by Kaspersky Security Center in the **Notifications** and **Exclusions from task scope** sections. For detailed information on configuring settings in these sections, see *Kaspersky Security Center Help*.

Application Integrity Control

To configure the Application Integrity Control group task:

1. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node and select the administration group for which you want to configure the application tasks.
2. In the details pane of a selected administration group, open the **Tasks** tab.
3. In the list of previously created group tasks, select a task you want to configure.
4. Open the **Properties: <Task name>** window in one of the following ways:
   - Double-click the name of the task in the list of created tasks.
   - Select the name of the task in the list of created tasks and click the **Configure task** link.
   - Open the context menu of the task name in the list of created tasks and select the **Properties** item.
5. In the **Notification** section, configure the task event notification settings. For detailed information on configuring settings in this section, see *Kaspersky Security Center Help*.
6. In the **Devices** section, select the devices for which you want to configure the Application Integrity Control task.
7. Configure the task schedule in the **Schedule** section (you can configure a schedule for all task types except Rollback of Database Update).
8. In the **Account** section, specify the account whose rights will be used to run the task.
9. If required, specify the objects to exclude from the task scope in the **Exclusions from task scope** section.

   For detailed information on configuring settings in these sections, see *Kaspersky Security Center Help*.

10. Click the **OK** button in the **Properties: <Task name>** window.

    The newly configured group task settings are saved.

Configuring crash diagnostics settings in Kaspersky Security Center

If a problem occurs when operating Kaspersky Embedded Systems Security for Windows (for example, the application crashes), you can diagnose it. To do this, you can enable the creation of trace files and a dump file for the Kaspersky Embedded Systems Security for Windows process and send these files for analysis to Technical Support.

Kaspersky Embedded Systems Security for Windows does not send any trace or dump files automatically. Diagnostic data can only be sent by a user who has the required permissions.

Kaspersky Embedded Systems Security for Windows writes information to trace files and the dump file in unencrypted form. The folder where files are saved is selected by the user and managed by the operating system configuration and Kaspersky Embedded Systems Security for Windows settings. You can configure access permissions and allow only required users to access logs, trace files and dump files.

To configure crash diagnostics settings in Kaspersky Security Center:

1. In the Kaspersky Security Center Administration Console, open the **Application settings** window.
2. Open the **Malfunction diagnosis** section.
3. To log debug information to a file, in the **Troubleshooting settings** section, select the **Enable tracing** check box.
4. In the **Trace files folder** field, specify the absolute path to the local folder where Kaspersky Embedded Systems Security for Windows will save trace files.

   The folder must be created in advance and be writable by the SYSTEM account. You cannot specify a network folder, drive, or environment variables.
5. Configure the level of detail of debug information.
6. Specify the **Maximum size of trace files (MB)**.

   Available values: from 1 to 4095 MB. By default, the maximum size of trace files is 50 MB.
7. To delete the oldest trace files when the maximum number of files is reached, select the **Remove older trace files** check box.
8. Specify the **Maximum number of files for one trace log**.

   Available values: from 1 to 999. By default, the maximum number of files is 5. The field is available if the **Remove the oldest trace files** check box is selected.
9. If you want the application to create a dump file, select the **Create dump file** check box.
10. In the **Dump files folder** field, specify the absolute path to the local folder where Kaspersky Embedded Systems Security for Windows will save dump files.

    The folder must be created in advance and be writable by the SYSTEM account. You cannot specify a network folder, drive, or environment variables.
11. Click the **OK** button.

The configured application settings are applied on the protected device.

Managing task schedules

You can schedule Kaspersky Embedded Systems Security for Windows tasks.

Scheduling tasks

You can schedule local system and custom tasks in the Application Console. You cannot schedule group tasks in the Application Console.

To schedule group tasks using the Administration Plug-in:

1. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node.
2. Select the group that the protected device belongs to.
3. In the results pane, select the **Tasks** tab.
4. Open the **Properties: <Task name>** window in one of the following ways:
   - Double-click the name of the task.
   - Open the context menu of the task name and select the Properties item.
5. Select the **Schedule** section.
6. In the **Schedule settings** block, select the **Run by schedule** check box.

   Fields with schedule settings for the On-Demand Scan and Update tasks are unavailable if scheduling of these tasks is blocked by a Kaspersky Security Center policy.

7. Configure schedule settings in accordance with your requirements. To do this, perform the following actions:
   a. in the **Frequency** list, select one of the following values:
      - **Hourly**, if you want the task to run at intervals of a specified number of hours; specify the number of hours in the **Every <number> hour(s)** field.
      - **Daily**, if you want the task to run at intervals of a specified number of days; specify the number of days in the **Every <number> day(s)** field.
      - **Weekly**, if you want the task to run at intervals of a specified number of weeks; specify the number of weeks in the **Every <number> week(s)** field. Specify the days of the week on which the task will be started (by default tasks run on Mondays).
      - **At application launch**, if you want the task to run every time Kaspersky Embedded Systems Security for Windows starts.
      - **After application database update**, if you want the task to run after every update of the application databases.
   b. Specify the time for the first task start in the **Start time** field.
   c. In the **Start date** field, specify the date when the schedule starts.

After you have scheduled the start time, date and frequency of the task, the estimated time for the next start is displayed.

Go to the **Schedule** tab and open the **Task settings** window. In the **Next start** field in the top of the window, the estimated start time is displayed. Each time you open the window, this estimated start time is updated and displayed.

The **Next start** field displays the **Blocked by policy** value if Kaspersky Security Center active policy settings prohibit scheduled local system tasks from starting.

8. Use the **Advanced** tab to configure the following schedule settings in accordance with your requirements.
   - In the **Task stop settings** section:
     a. Select the **Duration** check box and, in the fields to the right, enter the maximum number of hours and minutes of task execution.
     b. Select the **Pause from** check box and, in the fields to the right, enter the start and end values of a time interval under 24 hours during which task execution will be paused.
   - In the **Advanced settings** block:
     a. Select the **Cancel schedule from** check box and specify the date from which the schedule will cease to apply.
     b. Select the **Run skipped tasks** check box to enable the start of skipped tasks.
     c. Select the **Randomize the task start time within the interval of** check box and specify a value in minutes.
9. Click the **OK** button.
10. Click the **Apply** button to save the task start settings.

If you want to configure application settings for a single task using Kaspersky Security Center, see section "Configuring local tasks in the Application settings window of the Kaspersky Security Center".

Enabling and disabling scheduled tasks

You can enable and disable scheduled tasks either before or after configuring the schedule settings.

To enable or disable the task start schedule:

1. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node.
2. Select the group that the protected device belongs to.

3. In the results pane, select the **Tasks** tab.
4. Open the **Properties: <Task name>** window in one of the following ways:
   - Double-click the name of the task.
   - Open the context menu of the task name and select the Properties item.
5. Select the **Schedule** section.
6. Do one of the following:
   - Select the **Run by schedule** check box if you want to enable scheduled task start.
   - Clear the **Run by schedule** check box if you want to disable scheduled task start.

     The configured task start schedule settings are not deleted and will be applied at the next time you enable a scheduled task start.
7. Click the **OK** button.
8. Click the **Apply** button.

The configured task start schedule settings are saved.

Reports in Kaspersky Security Center

Reports in Kaspersky Security Center contain information about the status of managed devices. Reports are based on information stored on Administration Server.

Starting from Kaspersky Security Center 11, the following types of reports are available for Kaspersky Embedded Systems Security for Windows:

- Report on the status of application components
- Report on prohibited applications
- Report on prohibited applications in test mode

See *Kaspersky Security Center Help* for detailed information about all Kaspersky Security Center reports and how to configure them.

Report on the status of Kaspersky Embedded Systems Security for Windows components

You can monitor the protection status of all network devices and get a structured overview of the set of components on each device.

The report displays one of the following states for each component: *Running*, *Paused*, *Stopped*, *Malfunction*, *Not installed*, *Starting*.

Not Installed status refers to the component, not the application itself. If the application is not installed, Kaspersky Security Center assigns the N/A (Not available) status.

You can create component selections and use filtering to display network devices with a specified set of components and state.

See *Kaspersky Security Center Help* for detailed information about creating and using selections.

To review the component statuses in the application settings:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree and select the administration group for which you want to configure application settings.
2. Select the **Devices** tab and open the **Application settings** window.
3. Select the **Components** section.
4. Review the status table.

To review a Kaspersky Security Center standard report:

1. Select the **Administration Server <Administration Server name>** node in the Administration Console tree.
2. Open the **Reports** tab.
3. Double-click the **Report on the status of application components** list item.

   A report is generated.
4. Review the following report details:
   - A graphical diagram.
   - A summary table of components and aggregated numbers of network devices where each of the components is installed, and groups they belong to.
   - A detailed table specifying the component status, version, device and group.

Reports on prohibited applications in active and test modes

Based on the results of the Applications Launch Control task, two types of reports can be generated: a report on prohibited applications (if the task is started in Active mode) and a report on prohibited applications in test mode (if the task is started in Statistics only mode). These reports display information about blocked applications on the protected devices of the network. Each report is generated for all administration groups and accumulates data from all the Kaspersky applications installed on the protected devices.

To review a report on prohibited applications in Statistics only mode:

1. Start the Applications Launch Control task in Statistics only mode.

Select the **Administration Server <Administration Server name>** node in the Administration Console tree.

1. Open the **Reports** tab.

2. Double-click the **Report on prohibited applications in test mode** item.

   A report is generated.

3. Review the following report details:

   - A graphical diagram that displays the top 10 applications with the largest number of blocked starts.
   - A summary table of application blocks, specifying the executable file name, reason, time of blocking, and number of devices where the blocking occurred.
   - A detailed table specifying data about the device, file path and criteria for blocking.

To review a report on prohibited applications in Active mode:

1. Start the Applications Launch Control task in Active mode.
2. Select the **Administration Server <Administration Server name>** node in the Administration Console tree.
3. Open the **Reports** tab.
4. Double-click the **Report on prohibited applications** item.

   A report is generated.

This report consists of the same data about blocks as the report on prohibited applications in test mode.

Working with the Kaspersky Embedded Systems Security for Windows Console

This section provides information about the Kaspersky Embedded Systems Security for Windows Console and describes how to manage the application using the Application Console installed on the protected device or another device.

About the Kaspersky Embedded Systems Security for Windows Console

Kaspersky Embedded Systems Security for Windows Console is an isolated snap-in that you can add to the Microsoft Management Console.

You can manage the application via the Application Console installed on the protected device or on another device on the corporate network.

After the Application Console has been installed on another device, advanced configuration is required.

You can install the Application Console and Kaspersky Embedded Systems Security for Windows on different protected devices assigned to different domains. In this case, there may be limitations on sending information from the application to the Application Console. For example, after any application task starts, its status may remain unchanged in the Application Console.

When installing the Application Console, the installation wizard creates the kavfs.msc file in the installation folder and adds Kaspersky Embedded Systems Security for Windows snap-in to the list of isolated Microsoft Windows snap-ins.

You can start the Application Console from the **Start** menu. The Kaspersky Embedded Systems Security for Windows snap-in msc-file can be run or added to the Microsoft Management Console as a new element in the tree.

Under a 64-bit version of Microsoft Windows, the Kaspersky Embedded Systems Security for Windows snap-in can be added only in the 32-bit version of Microsoft Management Console. To add the Kaspersky Embedded Systems Security for Windows snap-in, open Microsoft Management Console from the command line by executing the command: mmc.exe /32.

Multiple Kaspersky Embedded Systems Security for Windows snap-ins can be added to one Microsoft Management Console opened in author mode. You can then manage the protection of multiple devices on which Kaspersky Embedded Systems Security for Windows is installed.

Kaspersky Embedded Systems Security for Windows Console interface

This section describes the primary elements of the application interface.

Kaspersky Embedded Systems Security for Windows Console window

The Kaspersky Embedded Systems Security for Windows Console is displayed as a node in the Microsoft Management Console tree.

After a connection has been established to Kaspersky Embedded Systems Security for Windows installed on a different protected device, the name of the node is supplemented with the name of the protected device on which the application is installed and the name of the user account under which the connection has been established: **Kaspersky Embedded Systems Security <Name of protected device> as <account name>**. When connecting to Kaspersky Embedded Systems Security for Windows installed on the same protected device with the Application Console, the node name is **Kaspersky Embedded Systems Security for Windows**.

The Application Console tree

The Application Console tree displays the **Kaspersky Embedded Systems Security for Windows** node and the child nodes of functional components of the application.

The **Kaspersky Embedded Systems Security for Windows** node includes the following child nodes:

- **Real-Time Computer Protection**: manages the Real-Time Computer Protection tasks and KSN services. The **Real-Time Computer Protection** node allows to configure the following tasks:
  - **Real-Time File Protection**
  - **KSN Usage**
  - **Exploit Prevention**
- **Computer Control**: control of applications running on the protected device and connected devices. The **Computer Control** node allows to configure the following tasks:
  - **Applications Launch Control**
  - **Device Control**
  - **Firewall Management**
- **Automated rule generators**: configuring automatic generation of group and system rules for the Applications Launch Control task and the Device Control task.
  - **Rule Generator for Applications Launch Control**
  - **Rule Generator for Device Control**
  - Rule generation group tasks **<Task names>** (if any)

    Group tasks are created using Kaspersky Security Center. You cannot manage group tasks through the Application Console.
- **System Inspection**: configuring file operations control and Windows Event Log inspection settings.
  - **File Integrity Monitor**
  - **Log Inspection**
- **On-Demand Scan**: manages On-Demand Scan tasks. There is a separate node for each task:
  - **Scan at Operating System Startup**

- **Critical Areas Scan**
- **Quarantine Scan**
- **Application Integrity Control**
- Custom tasks **<Task names>** (if any)

The node displays system tasks created when the application is installed, custom tasks, and group on-demand scan tasks created and sent to a protected device using Kaspersky Security Center.

- **Update**: manages updates for Kaspersky Embedded Systems Security for Windows databases and modules and copies the update to a local update source folder. The node contains child nodes for administering each update task and the last **Rollback of Application Database Update** task:
  - **Database Update**
  - **Software Modules Update**
  - **Copying Updates**
  - **Rollback of Application Database Update**

  The node displays all custom and group update tasks created and sent to a protected device using Kaspersky Security Center.
- **Storages**: Management of Quarantine and Backup settings.
  - **Quarantine**
  - **Backup**
- **Logs and notifications**: manages local task logs, Security log and Kaspersky Embedded Systems Security for Windows System audit log.
  - **Security log**
  - **System audit log**
  - **Task logs**
- **Licensing**: add or delete Kaspersky Embedded Systems Security for Windows keys, view license details.

Details pane

The details pane displays information about the selected node. If the **Kaspersky Embedded Systems Security for Windows** node is selected, the details pane displays information about the current device protection status and information about Kaspersky Embedded Systems Security for Windows, the protection status of its functional components, and the license expiration date.

Context menu of the Kaspersky Embedded Systems Security for Windows node

You can use the items of the context menu of the **Kaspersky Embedded Systems Security for Windows** node to perform the following operations:

- **Connect to another computer**. Connect to another device to manage Kaspersky Embedded Systems Security for Windows installed on it. You can also perform this operation by clicking the link in the lower right corner of the details pane of the **Kaspersky Embedded Systems Security for Windows** node.
- **Start the service** / **Stop the service**. Start or stop application or a selected task. To carry out these operations, you can also use the buttons on the toolbar. You can also perform these operations in context menus of application tasks.
- **Configure removable drives scan settings**. Configure scanning of removable drives connected to the protected device via the USB port.
- **Configure Trusted Zone settings**. View and configure Trusted Zone settings.
- **Modify user rights of application management**. View and configure permissions to access Kaspersky Embedded Systems Security for Windows functions.
- **Modify user rights of Kaspersky Security Service management**. View and configure user rights to manage Kaspersky Security Service.
- **Export settings**. Save the application settings in a configuration file in XML format. You can also perform this operation in context menus of application tasks.
- **Import settings**. Import application settings from a configuration file in XML format. You can also perform this operation in context menus of application tasks.
- **Information about the application and available module updates**. See information about Kaspersky Embedded Systems Security for Windows and currently available software module updates.
- **Refresh**. Refresh the contents of the Application Console window. You can also perform this operation in context menus of application tasks.
- **Properties**. View and configure settings of Kaspersky Embedded Systems Security for Windows or a selected task. You can also perform this operation in context menus of application tasks.

  To do so, you can also use the **Application properties** link in the details pane of the **Kaspersky Embedded Systems Security for Windows** node or use the button on the toolbar.

- **Help**. View information in Kaspersky Embedded Systems Security for Windows Help. You can also perform this operation in context menus of application tasks.

Toolbar and context menu of Kaspersky Embedded Systems Security for Windows tasks

You can manage Kaspersky Embedded Systems Security for Windows tasks using the context menus of each task in the Application Console tree.

You can use the items of the context menu to perform the following operations:

- **Start** / **Stop**. Start or stop task execution. To carry out these operations, you can also use the buttons on the toolbar.
- **Resume** / **Pause**. Resume or pause task execution. To carry out these operations, you can also use the buttons on the toolbar. This operation is available for the Real-Time Computer Protection tasks and the On-Demand Scan tasks.

- **Add task**. Create new custom task. This operation is available for On-demand scan tasks.
- **Open log**. View and manage the task log. This operation is available for all tasks.
- **Remove task**. Delete custom task. This operation is available for On-demand scan tasks.
- **Settings templates**. Manage templates. This operation is available for Real-Time File Protection and On-Demand Scan.

System Tray Icon in the notification area

Every time Kaspersky Embedded Systems Security for Windows automatically starts after a protected device restart, the System Tray Icon is displayed in the toolbar notification area . It is displayed by default if the System Tray Icon component was installed during application setup.

The appearance of the System Tray Icon reflects the current device protection status. There are two types of status:

	Active (colored icon) if at least one task is running: Real-Time File Protection, Applications Launch Control.
	Inactive (gray icon) – none of the following tasks are currently running: Real-Time File Protection and Applications Launch Control

You can open the context menu of the System Tray Icon by right-clicking it.

The context menu offers several commands to display application windows (see table below).

Context menu commands in System Tray Icon

Command	Description
Open the Application Console	Opens Kaspersky Embedded Systems Security for Windows Console (if installed).
Open Compact Diagnostic Interface	Opens the Compact Diagnostic Interface.
About the application	Opens the **About the application** window containing information about Kaspersky Embedded Systems Security for Windows. For registered Kaspersky Embedded Systems Security for Windows users, the **About the application** window contains information about urgent updates that have been installed.
Hide	Hides the System Tray Icon in the toolbar notification area.

You can display the hidden System Tray Icon again at any time.

To display the System Tray Icon again,

in the Microsoft Windows **Start** menu, select **All Programs** > **Kaspersky Embedded Systems Security for Windows** > **System Tray Icon**.

The names of settings may vary depending on the installed operating system.

In the general settings of Kaspersky Embedded Systems Security for Windows, you can enable or disable the display of the System Tray Icon every time the application starts automatically following a protected device restart.

Managing Kaspersky Embedded Systems Security for Windows via the Application Console on another device

You can manage Kaspersky Embedded Systems Security for Windows via the Application Console installed on a remote device.

To manage the application using Kaspersky Embedded Systems Security for Windows Console on a remote device, make sure that:

- The Application Console users on the remote device are added to the ESS Administrators group on the protected device.
- Network connections are allowed for the Kaspersky Security Management Service process (kavfsgt.exe) if Windows Firewall is enabled on the protected device.
- During installation of Kaspersky Embedded Systems Security for Windows, the **Allow remote access** check box is selected in the Installation Wizard window.

If Kaspersky Embedded Systems Security for Windows on the remote device is password protected, enter the password to access application management via the Application Console.

Configuring general application settings via the Application Console

General settings and malfunction diagnostics settings of Kaspersky Embedded Systems Security for Windows establish the general operating conditions for the application. These settings allow you to control the number of working processes used by Kaspersky Embedded Systems Security for Windows, enable recovery of Kaspersky Embedded Systems Security for Windows tasks after an abnormal termination, maintain the log, enable creation of dump files of Kaspersky Embedded Systems Security for Windows processes after abnormal termination, and configure other general settings.

Application settings cannot be configured in the Application Console if the active Kaspersky Security Center policy blocks changes to these settings.

To configure Kaspersky Embedded Systems Security for Windows settings:

1. In the Application Console tree, select the **Kaspersky Embedded Systems Security for Windows** node and do one of the following:
   - Click the **Application properties** link in the details pane of the node.
   - Select **Properties** in the node's context menu.

The **Application settings** window is displayed.

2. In the window that opens, configure Kaspersky Embedded Systems Security for Windows general settings according to your preferences:

   - The following settings can be configured on the **Scalability and interface** tab:

     - In the **Scalability settings** section:

       - Number of processes for Real-Time Computer Protection

       - Number of working processes for background On-Demand Scan tasks

   - In the **Interaction with user** section select if the System Tray Icon will be displayed in the taskbar after each application start.

   - The following settings can be configured on the **Security and reliability** tab:

     - In the **Password protection settings** section, configure the protection of application processes.

     - In the **Password protection settings** section, configure the settings for password-protection of the application's functions.

     - In the **Self-defense** section, specify the number of attempts to recover an On-Demand Scan task if it crashes.

   - In the **Recover on-demand scan tasks no more than (times)** section, specify actions that Kaspersky Embedded Systems Security for Windows performs when switching to UPS power.

   - On the **Scan settings** tab:

     - **Restore file attributes after scanning**

     - **Limit CPU usage for scanning threads**

     - **Upper limit (per cent)**

     - **Folder for temporary files created during scanning**

   - On the **Connection settings** tab:

     - In the **Proxy server settings** section, specify the proxy server settings.

     - In the **Proxy server authentication settings** section, specify the authentication type and details required for authentication on the proxy server.

     - In the **Licensing** section, indicate whether Kaspersky Security Center will be used as a proxy-server for application activation.

   - On the **Malfunction diagnosis** tab:

     - If you want the application to write debug information to a file, in the **Troubleshooting settings** subsection, select the **Enable tracing** check box.

     - In the **Trace folder** field, specify the absolute path to the local folder where Kaspersky Embedded Systems Security for Windows will save trace files.

The folder must be created in advance and be writable by the SYSTEM account. You cannot specify a network folder, drive, or environment variables.

- Configure the level of detail of debug information.
- Specify the **Maximum size of trace files**.

  Available values: from 1 to 4095 MB. By default, the maximum size of trace files is 50 MB.
- If you want the application to remove the oldest files after the maximum number of trace files is reached, select the **Remove the oldest trace files** check box.
- Specify the **Maximum number of files for one trace log**.

  Available values: from 1 to 999. By default, the maximum number of files is 5. The field is available only if the **Remove the oldest trace files** check box is selected.
- If you want the application to create a dump file, select the **Create dump file** check box.
- In the **Dump file folder** field, specify the absolute path to the local folder where Kaspersky Embedded Systems Security for Windows will save dump files.

  The folder must be created in advance and be writable by the SYSTEM account. You cannot specify a network folder, drive, or environment variables.

Kaspersky Embedded Systems Security for Windows writes information to trace files and the dump file in unencrypted form. The folder where files are saved is selected by the user and managed by the operating system configuration and Kaspersky Embedded Systems Security for Windows settings. You can configure access permissions and allow only required users to access logs, trace files and dump files.

3. Click the **OK** button.

Kaspersky Embedded Systems Security for Windows settings are saved.

Managing Kaspersky Embedded Systems Security for Windows tasks

This section contains information about how to create, configure, start, and stop Kaspersky Embedded Systems Security for Windows tasks.

Kaspersky Embedded Systems Security for Windows task categories

Real-Time Computer Protection, Computer Control, On-Demand Scan, and Update functions in Kaspersky Embedded Systems Security for Windows are implemented as tasks.

You can manage these tasks using the task context menu in the Application Console tree, the toolbar, and the quick access bar. You can view task status information in the results pane. Task management operations are recorded in the system audit log.

There are two types of Kaspersky Embedded Systems Security for Windows tasks: *local* and *group*.

Local tasks

Local tasks can only be executed on the protected device they were created for. Depending on the start method, the following types of local tasks exist:

- **Local system tasks**. These tasks are created automatically during installation of Kaspersky Embedded Systems Security for Windows. You can edit the settings of all local system tasks, except for the Quarantine Scan and Rollback of Database Update tasks. Local system tasks cannot be renamed or deleted. You can run local system and custom On-Demand Scan tasks simultaneously.

- **Local custom tasks**. In the Application Console, you can create On-Demand Scan tasks. In Kaspersky Security Center, you can create On-Demand Scan, Database Update, Rollback of Database Update, and Copying Updates tasks. You can rename, configure, and delete custom tasks. You can run several custom tasks simultaneously.

Group tasks

You can manage group tasks and tasks for sets of protected devices from the Kaspersky Security Center. All group tasks are custom tasks. Group tasks are also displayed in the Application Console. In the Application Console, you can only view the status of group tasks. You cannot use the Application Console to manage or configure group tasks.

Starting, pausing, resuming, and stopping tasks manually

You can pause and resume only Real-Time Computer Protection and On-Demand Scan tasks. No other tasks can be paused or resumed manually.

To start, pause, resume or stop a task:

1. In the Application Console, open the context menu of the task.

2. Select one of the following commands: **Start**, **Pause**, **Resume**, or **Stop**.

   The operation is performed and recorded in the system audit log.

When you resume an On-Demand Scan task, Kaspersky Embedded Systems Security for Windows resumes scanning from the object on which the scan was paused.

Managing task schedules

You can schedule Kaspersky Embedded Systems Security for Windows tasks.

Configuring the task schedule settings

In the Application Console, you can schedule when to start local system and custom tasks. However, you cannot schedule when to start group tasks.

To schedule a task:

1. Open the context menu of the task you want to schedule.
2. Select **Properties**.

   The **Task settings** window appears.
3. In the window that opens, on the **Schedule** tab, select the **Run by schedule** check box.
4. Follow these steps to specify schedule settings:

   a. In the **Frequency** drop-down menu, select one of the following:

   - **Hourly**: to run the task at some interval measured in hours; specify the number of hours in the **Every <number> hour(s)** field.
   - **Daily**: to run the task at some interval measured in days; specify the number of days in the **Every <number> day(s)** field.
   - **Weekly**: to run the task at some interval measured in weeks; specify the number of weeks in the **Every <number> week(s) on** field. Specify the days of the week on which the task will be started (by default tasks run on Mondays).
   - **At application launch**, if you want the task to run every time Kaspersky Embedded Systems Security for Windows starts.
   - **After application database update**, if you want the task to run after every update of the application databases.

   b. Specify the time for the first task start in the **Start time** field.

   c. In the **Start date** field, specify the date when to start the task for the first time.

   After you have specified the task start frequency, the time of the first task start, and the date from which the schedule applies, the estimated time for the next task start will appear in the top part of the window in the **Next start** field. The estimated time of the next task start will be updated and displayed each time you open the **Task settings** window on the **Schedule** tab.

   The **Next start** field displays the **Blocked by policy** value if Kaspersky Security Center active policy settings prohibit scheduled local system tasks from starting.
5. Use the **Advanced** tab to specify the following schedule settings:

   - In the **Task stop settings** section:

     a. Select the **Duration** check box. In the fields to the right, enter maximum task duration in hours and minutes.

     b. Select the **Pause from** check box. In the fields to the right, enter when to pause and resume the task (under 24 hours).

   - In the **Advanced settings** block:

     a. Select the **Cancel schedule from** check box and specify the task schedule end date.

b. Select the **Run skipped tasks** check box to start skipped tasks.

c. Select the **Randomize the task start within interval of** check box and specify a value in minutes.

6. Click the **OK** button.

The task schedule settings are saved.

Enabling and disabling scheduled tasks

You can enable and disable scheduled tasks either before or after configuring the schedule settings.

To enable or disable a scheduled task start:

1. In the Application Console tree, open the context menu for the scheduled task.
2. Select **Properties**.
   The **Task settings** window appears.
3. In the window that opens, on the **Schedule** tab, select one of the following options:
   - Select the **Run by schedule** check box if you want to enable scheduled task start.
   - Clear the **Run by schedule** check box if you want to disable scheduled task start.

     The task start schedule settings are not deleted and will be applied the next time you enable a scheduled task start.
4. Click the **OK** button.

The task schedule settings are saved.

Using user accounts to start tasks

You can start tasks under the system account or specify a different account.

About using accounts to start tasks

You can specify the account to run the following Kaspersky Embedded Systems Security for Windows tasks:

- Rule Generator for Applications Launch Control
- Rule Generator for Device Control
- On-Demand Scan
- Update

By default, these tasks are run using system account permissions.

A different account with proper access permissions is recommended in the following cases:

- **Update** task: if you specified a shared folder on a different device on the network as the update source.
- **Update** task: if you use a proxy server with built-in Windows NTLM authentication to access the update source.
- **On-Demand Scan** tasks: if the system account does not have permission to access the scanned objects (for example, files in shared folders on the protected device).
- **Rule Generator for Applications Launch Control** task: if the generated rules are exported to a configuration file that the system account cannot access (for example, in a shared folder on the protected device).

You can run Update, On-Demand Scan, and Rule Generator for Applications Launch Control tasks with system account permissions. Kaspersky Embedded Systems Security for Windows performs these tasks and accesses shared folders on another device in the network if this device is registered in the same domain as the protected device. In this case, the system account must have access permissions for these folders. Kaspersky Embedded Systems Security for Windows accesses the device using permissions for the account **<domain name \ device_name>**.

Specifying a user account to start a task

To specify an account to start a task:

1. In the Application Console tree, open the context menu of the task you want to start by using a specific account.
2. Select **Properties**.

   The **Task settings** window appears.
3. In the window that opens, on the **Run as** tab, follow these steps:

   a. Select **User name**.

   b. Enter the user name and password for the account you want to use.

   The selected user must be registered on the protected device or in the same domain as this computer.

   c. Confirm the password.
4. Click the **OK** button.

The modified settings are saved.

Importing and exporting settings

This section explains how to export Kaspersky Embedded Systems Security for Windows settings. You will also learn how to export specific software settings to an XML configuration file, and how to import these settings from a configuration file back into the application.

About importing and exporting settings

You can export Kaspersky Embedded Systems Security for Windows settings to an XML configuration file and import settings into Kaspersky Embedded Systems Security for Windows from the configuration file. You can save all application settings or only settings for individual components to a configuration file.

When you export all settings of Kaspersky Embedded Systems Security for Windows to a file, the general application settings and settings of the following Kaspersky Embedded Systems Security for Windows components and functions are saved:

- Real-Time File Protection
- KSN Usage
- Device Control
- Applications Launch Control
- Rule Generator for Device Control
- Rule Generator for Applications Launch Control
- On-Demand Scan tasks
- File Integrity Monitor
- Log Inspection
- Kaspersky Embedded Systems Security for Windows database and software modules update
- Quarantine
- Backup
- Logs
- Administrator and user notifications
- Trusted zone
- Exploit Prevention
- Password protection

Also, you can save the general settings of Kaspersky Embedded Systems Security for Windows in the file, as well as the rights of user accounts.

You cannot export group task settings.

Kaspersky Embedded Systems Security for Windows exports all passwords used by the application, for example, user account settings for running tasks or connecting to a proxy server. Exported passwords are saved in encrypted form in the configuration file. You can import passwords only using Kaspersky Embedded Systems Security for Windows installed on this protected device if it has not been reinstalled or updated.

You cannot import previously saved passwords using Kaspersky Embedded Systems Security for Windows installed on a different protected device. After settings have been imported on the protected device, all passwords must be entered manually.

If a Kaspersky Security Center policy is active at the time of export, the application exports the specified values used by that policy.

Settings can be imported from a configuration file containing settings for individual Kaspersky Embedded Systems Security for Windows components (e.g. from a file created in Kaspersky Embedded Systems Security for Windows installed with an incomplete set of components). After the settings are imported, only those Kaspersky Embedded Systems Security for Windows settings that were contained in the configuration file are changed. All other settings remain the same.

Settings of an active Kaspersky Security Center policy that have been blocked do not change when importing the settings.

Exporting settings

To export settings to a configuration file:

1. In the Application Console tree, do one of the following:

   - In the context menu of the **Kaspersky Embedded Systems Security for Windows** node, select **Export settings** to export all Kaspersky Embedded Systems Security for Windows settings.
   - In the context menu of a specific task, select **Export settings** to export the settings of an individual functional component of the application.
   - To export the Trusted Zone settings:

     a. In the Application Console tree, open the context menu of the **Kaspersky Embedded Systems Security for Windows** node.

     b. Select **Configure Trusted Zone settings**.

     The **Trusted Zone** window opens.

     c. Click the **Export** button.

     The Settings Export Wizard opens.

2. Follow the instructions in the **Settings Export Wizard**: specify the name and path of the configuration file you want to use to save the settings.

   You can use system environment variables when specifying the path, but not user environment variables.

   If a Kaspersky Security Center policy is active at the time of export, the application exports the settings used by that policy.

3. Click the **Export of application settings complete** button in the **Close** window.

The Settings Export Wizard closes and saves the export settings.

Importing settings

To import settings from a saved configuration file:

1. In the Application Console tree, do one of the following:

   - In the context menu of the **Kaspersky Embedded Systems Security for Windows** node, select **Import settings** to import all Kaspersky Embedded Systems Security for Windows settings.
   - In the context menu of a specific task, select **Import settings** to import the settings of an individual functional component of the application.
   - To import the Trusted Zone settings:

     a. In the Application Console tree, open the context menu of the **Kaspersky Embedded Systems Security for Windows** node.

     b. Select **Configure Trusted Zone settings**.

     The **Trusted Zone** window opens.

     c. Click the **Import** button.

     The Settings Import Wizard opens.

2. Follow the instructions in the **Settings Import Wizard**: specify the configuration file with the settings you want to import.

   After importing the general Kaspersky Embedded Systems Security for Windows settings or its functional component settings to the protected device, you cannot revert to the previous settings.

3. Click the **Application settings import completed** button in the **Close** window.

   The Settings Import Wizard closes and saves the imported settings.

4. In the Application Console toolbar, click the **Refresh** button.

The Application Console window displays the imported settings.

Kaspersky Embedded Systems Security for Windows does not import passwords (account credentials for starting tasks or connecting to the proxy server) from a file created on another protected device or on the same protected device after Kaspersky Embedded Systems Security for Windows has been re-installed or updated on it. After import is complete, passwords must be entered manually.

Using security settings templates

This section contains information about using security settings templates in Kaspersky Embedded Systems Security for Windows protection and scan tasks.

About security settings templates

You can manually configure the security settings of a node in the tree or in a list of the protected device's file resources, and save the configured setting values as a template. This template can then be used to specify the security settings of other nodes in Kaspersky Embedded Systems Security for Windows protection and scan tasks.

You can use templates to specify the security settings of the following Kaspersky Embedded Systems Security for Windows tasks:

- Real-Time File Protection
- Scan at Operating System Startup
- Critical Areas Scan
- On-Demand Scan tasks

Security settings from a template applied to a parent node in the protected device's file resource tree are applied to all child nodes. The parent node template is not applied to child nodes in the following cases:

- If you specified the security settings of the child nodes separately.
- If the child nodes are virtual. In this case, you must apply the template to each virtual node separately.

Creating a security settings template

To manually save the security settings of a node to a template:

1. In the Application Console tree, select the task for which you want to create a security settings template.
2. In the details pane of the selected task, click the **Configure protection scope** or **Configure scan scope** link.
3. In the tree or list of the protected device's network file resources, select the template that you want to view.
4. On the **Security level** tab, click the **Save as template** button.
   The **Template properties** window opens.
5. In the **Template name** field, enter the name of the template.
6. In the **Description** field, enter additional template information.
7. Click the **OK** button.

The security settings template is saved.

Viewing security settings in a template

To view security settings in a template that you created:

1. In the Application Console tree, select the task with the security settings template want to view.
2. In the context menu of the selected task, select **Settings templates**.

   The **Templates** window opens.
3. In the list of templates, select the template that you want to view.
4. Click the **View** button.

The **<Template name>** window opens. The **General** tab displays the template name and additional information about the template. The **Options** tab lists security settings saved in the template.

Applying a security settings template

To apply security settings from a template to a selected node:

1. In the Application Console tree, select the task to which you want to apply a security settings template.
2. In the details pane of the selected task, click the **Configure protection scope** or **Configure scan scope** link.
3. In the tree or list of the protected device's network file resources, open the context menu of the node or item to which you want to apply the template.
4. Select **Apply template** → **<Template name>**.
5. Click the **Save** button.

This applies the security settings template to the selected node in the file resource tree of the protected device. The value on the **Security level** tab for the selected node changes to **Custom**.

If the security settings of a template are applied to a parent node in the protected device file resource tree, these settings are also applied to all child nodes.

You can configure the protection or scan scope of child nodes in the file resource tree of the protected device separately. In this case, the security settings of the template applied to the parent node are not automatically applied to the child nodes.

To apply security settings from a template to all selected nodes:

1. In the Application Console tree, select the task to which you want to apply a security settings template.
2. In the details pane of the selected task, click the **Configure protection scope** or **Configure scan scope** link.

3. In the tree or list of the protected device's network file resources, select a parent node to apply the template to the selected node and its child nodes.

4. In the context menu, select **Apply template** → **<Template name>**.

5. Click the **Save** button.

The security settings template is applied to the parent and all child nodes in the protected device's file resource tree. The value on the **Security level** tab for the selected node changes to **Custom**.

Deleting a security settings template

To delete a security settings template:

1. In the Application Console tree, select the task with the security settings template that you want to delete.

2. In the context menu of the selected task, select **Settings templates**.

   The **Templates** window opens.

   In the results pane of the **On-Demand Scan** parent node you can view settings templates for On-Demand Scan tasks.

3. In the list of templates, select the template that you want to delete.

4. Click the **Remove** button.

   A window opens to confirm deletion.

5. In the window that opens, click **Yes**.

The selected template is deleted.

You can apply the security settings template to protect or scan nodes in the file resource tree of the protected device. In this case, the security settings for such nodes are unchanged after the template is deleted.

Viewing protection status and Kaspersky Embedded Systems Security for Windows information

To view information about the device protection status Kaspersky Embedded Systems Security for Windows,

select the **Kaspersky Embedded Systems Security for Windows** node in the Application Console tree.

By default, information in the details pane of the Application Console is refreshed automatically:

- Every 10 seconds in case of a local connection.
- Every 15 seconds in case of a remote connection.

You can refresh information manually.

*To refresh information in the **Kaspersky Embedded Systems Security for Windows** node manually,*

select the **Refresh** command in the context menu of the **Kaspersky Embedded Systems Security for Windows** node.

The following application information is displayed in the details pane of the Application Console:

- Kaspersky Security Network Usage status.
- Device protection status.
- Information about database and application module updates.
- Actual diagnostics data.
- Data about protected device control tasks.
- License information.
- Status of integration with Kaspersky Security Center: details of the server with Kaspersky Security Center installed, to which the application is connected; information about application tasks controlled by the active policy.

Color coding is used to display the protection status:

- *Green*. The task is being run in accordance with the configured settings. Protection is active.
- *Yellow*. The task was not started, has been paused, or has been stopped. Security threats may occur. You are advised to configure and start the task.
- *Red*. The task completed with an error or a security threat was detected while the task was running. You are advised to start the task or take measures to eliminate the detected security threat.

Some details in this block (for example, task names or the number of threats detected) are links that, when clicked, take you to the node of the relevant task or open the task log.

The **Kaspersky Security Network Usage** section displays current task status, for example, *Running*, *Stopped* or *Never performed*. The indicator can take the following values:

- Green color signifies that the KSN Usage task is running and file requests for statuses are being send to KSN.
- Yellow color signifies that one of the Statements is accepted, but the task is not running; or the task is running, but file requests are not sent to KSN.

Computer protection

The **Computer protection** section (see the table below) displays information about the device's current protection status.

Information about device protection status

Protection section	Information

Device protection status indicator	The color of the panel with the section name reflects the status of tasks being performed in the section. The indicator can take the following values: • Green – This color is displayed by default and signifies that Real-Time File Protection component is installed and the task is running. • Yellow – The Real-Time File Protection component is not installed, and the Critical Areas Scan task has not been performed for a long time. • Red – Real-Time File Protection task is not running.
Real-Time File Protection	**Task status** – Current task status, for example, *Running* or *Stopped*. **Detected** – Number of objects detected by Kaspersky Embedded Systems Security for Windows. For example, if Kaspersky Embedded Systems Security for Windows detects the same malicious application in five files, the value in this field increases by one. If the number of detected malicious applications exceeds 0, the value is highlighted in red.
Critical Areas Scan	**Last scan date** – Date and time of the last Critical Areas Scan for viruses and other computer security threats. *Never performed* – an event that occurs when the Critical Areas Scan task has not been performed in the last 30 days or longer (default value). You can change the threshold for generating this event.
Exploit prevention	**Status** – current status of exploit prevention techniques, for example, *Applied* or *Not applied*. **Operating mode** – one of two available modes, selected during configuration of process memory protection: **Terminate on exploit** or **Statistics only**. **Processes protected** – the total number of processes added to the protection scope and handled in accordance with the selected mode.
Backed up objects	*Backup free space threshold exceeded* – This event occurs when the amount of free space in Backup is approaching the specified limit. Kaspersky Embedded Systems Security for Windows continues to move objects to Backup. In this case, the value in the **Space used** field is highlighted in yellow. *Maximum Backup size exceeded* – this event occurs when the Backup size has reached the specified limit. Kaspersky Embedded Systems Security for Windows continues to move objects to Backup. In this case, the value in the **Space used** field is highlighted in red. **Backed up objects** – Number of objects currently in Backup. **Space used** – amount of Backup space used.

Update

The **Update** section (see the table below) displays information about how current databases and application modules are.

Information about the status of Kaspersky Embedded Systems Security for Windows databases and modules

Update section	Information
Status indicator of databases and software modules	The color of the panel with the section name reflects the status of application databases and modules. The indicator can take the following values: • Green – This color is displayed by default and signifies that application databases are up to date and that the last database update task was completed successfully. • Yellow – Databases are out of date, or the last database update task failed.

	• Red – The event *Application database is extremely out of date* or *Application database is corrupted* has occurred.
Database Update and **Software Modules Update**	**Database status** – an evaluation of the Database Update status. The option can take the following values: • **Application database is up to date** – application databases were updated no more than 7 days ago (default). • **Application database is out of date** – application databases were updated between 7 and 14 days ago (default). • **Application database is extremely out of date** – Application databases were updated more than 14 days ago (default). You can change the thresholds for generating the *Application database is up to date* and *Application database is extremely out of date* events. **Database release date** – the date and time of release of the latest databases update. The date and time are specified in UTC format. **Status of the latest completed Database Update task** – Date and time of the latest database update. The date and time are specified according to the local time of the protected device. The field is red if the *Failed* event occurred. **Number of module updates available** – the number of Kaspersky Embedded Systems Security for Windows module updates available to be downloaded and installed. **Number of module updates installed** – the number of installed Kaspersky Embedded Systems Security for Windows module updates.

Control

The **Control** section (see table below) displays information about the Applications Launch Control, Device Control, and Firewall Management tasks.

Information about protected device control status

Control section	Information
Status indicator for protected device control	The color of the panel with the section name reflects the status of tasks being performed in the section. The indicator can take the following values: • Green – This color is displayed by default and signifies that the Applications Launch Control component is installed and the task is running in the **Active** mode. • Yellow – Applications Launch Control is running in the **Statistics only** mode. • Red – The Applications Launch Control task is not running or failed.
Applications Launch Control	**Task status** – Current task status, for example, *Running* or *Stopped*. **Operation mode** – one of the two available modes for the Applications Launch Control task: **Active** or **Statistics only**. **Applications launches denied** – the number of attempts to start applications blocked by Kaspersky Embedded Systems Security for Windows during the Applications Launch Control task. If the number of blocked application launches exceeds 0, the field is red.

	Average processing time (ms) – Time taken by Kaspersky Embedded Systems Security for Windows to process an attempt to start applications on the protected device.
Device control	**Task status** – Current task status, for example, *Running* or *Stopped*. **Operation mode** – one of the two available modes for the Device Control task: **Active** or **Statistics only**. **Devices blocked** – the number of attempts to connect an external device, that were blocked by Kaspersky Embedded Systems Security for Windows during the Device Control task. If the number of blocked external devices exceeds 0, the field value is colored in red.
Firewall Management	**Task status** – Current task status, for example, *Running* or *Stopped*. **Connection attempts blocked** – the number of connections to a protected device that were blocked by the specified firewall rules.

Diagnostics

The **Diagnostics** section (see the table below) displays information about the File Integrity Monitor and Log Inspection tasks.

Information about System Inspection status

Diagnostics section	Information
Diagnostics status indicator	The color of the panel with the section name reflects the status of tasks being performed in the section. The indicator can take the following values: • Green – This color is displayed by default and signifies that one or both system inspection components are installed and tasks are running. • Yellow – both components are installed, but one of the system inspection tasks is not running; the *Not running* event occurs. • Red – one of the tasks failed.
File Integrity Monitor	**Task status** – Current task status, for example, *Running* or *Stopped*. **Non-sanctioned file operations** – The number of changes to files within the monitoring scope. These changes may indicate that the security of a protected device has been breached.
Log Inspection	**Task status** – Current task status, for example, *Running* or *Stopped*. **Violations of the configured rules** – Number of recorded violations based on data from the Windows Event Log. This number is determined based on the specified task rules or using the heuristic analyzer.

The Kaspersky Embedded Systems Security for Windows licensing information is displayed in the row in the bottom-left corner of the details pane of the **Kaspersky Embedded Systems Security for Windows** node.

You can configure Kaspersky Embedded Systems Security for Windows properties by following the **Application properties** link.

You can connect to a different protected device by following the **Connect to another computer** link.

Working with the Web Plug-in from Web Console and Cloud Console

This section provides information about the Kaspersky Embedded Systems Security for Windows Administration Plug-in and describes how to manage the application installed on a protected device or on a group of protected devices.

Managing Kaspersky Embedded Systems Security for Windows from Web Console and Cloud Console

You can centrally manage several protected devices that have Kaspersky Embedded Systems Security for Windows installed and are joined in an administration group using the Kaspersky Embedded Systems Security for Windows Web Plug-in. Kaspersky Security Center Web Console and Kaspersky Security Center Cloud Console also allow you to separately configure the settings of each protected device included in an administration group.

An administration group is created manually on Kaspersky Security Center Web Console. The group includes several devices with Kaspersky Embedded Systems Security for Windows installed for which you want to configure the same control and protection settings. For details on using administration groups, see *Kaspersky Security Center Help*.

Application settings for a single protected device are unavailable if the operation of Kaspersky Embedded Systems Security for Windows on the protected device is controlled by an active Kaspersky Security Center policy.

Kaspersky Embedded Systems Security for Windows can be managed from Kaspersky Security Center Web Console in the following ways:

- **Using Kaspersky Security Center policies**. Kaspersky Security Center policies can be used to remotely configure the same protection settings for a group of devices. Task settings specified in the active policy have priority over task settings configured locally in the Application Console or remotely in the device properties window of Kaspersky Security Center Web Console. Policies can be used to configure general application settings, settings for real-time computer protection tasks, activity control tasks on devices, and settings for starting local system tasks on a schedule.

- **Using Kaspersky Security Center group tasks**. Kaspersky Security Center group tasks allow remote configuration of common settings of tasks with an expiration period for a group of devices. You can use group tasks to activate the application, configure On-Demand Scan task settings, update task settings, and Rule Generator for Applications Launch Control task settings.

- **Using tasks for a set of devices**. Tasks for a set of devices allow remote configuration of common task settings with a limited execution period for protected devices that do not belong to any administration group.

- **Using the properties window of a single device**. In the device properties window, you can remotely configure the task settings for a single protected device included in an administration group. You can also configure both general application settings and settings for all Kaspersky Embedded Systems Security for Windows tasks if the selected protected device is not controlled by an active Kaspersky Security Center policy.

Kaspersky Security Center Web Console and Kaspersky Security Center Cloud Console allow you to configure application settings and advanced features, and work with logs and notifications. You can configure these settings for a group of protected devices and for individual protected devices.

Web Plug-in limitations

Kaspersky Embedded Systems Security for Windows Web Plug-in has the following limitations compared to Kaspersky Embedded Systems Security for Windows Administration Plug-in:

- To add users or user groups, you need to specify the security descriptor strings using the security descriptor definition language (SDDL).
- Predefined security level cannot be changed for the Real-Time File Protection task.
- Application Launch Control task rules cannot be created using digital certificate or Kaspersky Security Center events.
- Device Control task rules cannot be generated based on connected devices or on system data.

Managing application settings

This section contains information about configuring Kaspersky Embedded Systems Security for Windows general settings in Kaspersky Security Center Web Console.

Configuring general application settings in Web Plug-in

You can configure Kaspersky Embedded Systems Security for Windows general settings in Web Plug-in for a group of protected devices or one protected device.

Configuring scalability, interface, and scan settings in Web Plug-in

To configure scalability settings and the application interface:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.
2. Click the policy name you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.
4. Select the **Application settings** section.
5. Click the **Settings** button in the **Scalability, interface and scan settings** subsection.
6. Configure the settings described in the table below.

Scalability settings

Setting	Description
Automatically detect scalability settings	Kaspersky Embedded Systems Security for Windows automatically controls the number of processes used. This is the default value.
Set the number of	Kaspersky Embedded Systems Security for Windows controls the number of active working processes according to the values specified.

working processes manually	
Number of processes for real-time protection	Maximum number of processes that are used by the Real-Time Computer Protection task components. The entry field is available if the **Set the number of working processes manually** option is selected.
Number of processes for background on-demand scan tasks	Maximum number of processes used by the On-Demand Scan component when running On-Demand Scan tasks in background mode. The entry field is available if the **Set the number of working processes manually** option is selected.
Display System Tray Icon in the taskbar	Configure whether the System Tray Icon will be displayed in the notification area.
Restore file attributes after scanning	When Kaspersky Embedded Systems Security for Windows performs On-Demand Scan and Real-Time File Protection tasks, the time when each scanned file was last accessed is updated. After the scan, Kaspersky Embedded Systems Security for Windows resets the time when the file was last accessed to the initial value. This behavior can affect the work of backup systems by causing creation of backup copies for files that haven't been changed. This can also cause false detections in file change tracking applications. By default, this function is enabled.
Limit CPU usage for scanning threads	Kaspersky Embedded Systems Security for Windows limits its use of the protected device CPU during on-demand scan tasks to the value specified in the **Upper limit (per cent)** field. Enabling of this option can negatively affect the performance of Kaspersky Embedded Systems Security for Windows. By default, this option is disabled.
Upper limit (in percentages)	Maximum allowable value of CPU utilization by Kaspersky Embedded Systems Security for Windows. The entry field is available if the **Limit CPU usage for scanning threads** option is selected.
Folder for temporary files created during scanning	Folder into which Kaspersky Embedded Systems Security for Windows needs to unpack archive files during scanning. By default, the C:\Windows\Temp folder is used.
HSM system settings	Select the option for accessing the hierarchical storage.

Configuring security settings in Web Plug-in

To configure security settings manually, take the following steps:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.
2. Click the policy name you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.
4. Select the **Application settings** section.
5. Click the **Settings** button in the **Security and reliability** subsection.
6. Configure the settings described in the table below.

Security settings

Setting	Description
Protect application processes from external threats	If the **Protect application processes from external threats** function is enabled, the application protects its processes against code injection and accessing of process data. When enabling or disabling this function, there is no need to restart the application services for the changes to apply. The function is enabled by default.
Perform task recovery	This check box enables or disables the recovery of Kaspersky Embedded Systems Security for Windows tasks when the application returns an error or terminates. If the check box is selected, Kaspersky Embedded Systems Security for Windows automatically recovers Kaspersky Embedded Systems Security for Windows tasks when the application returns an error or terminates. If the check box is cleared, Kaspersky Embedded Systems Security for Windows does not recover Kaspersky Embedded Systems Security for Windows tasks when the application returns an error or terminates. The check box is selected by default.
Recover On-Demand Scan tasks no more than (times) in range 1 - 10 attempts	The number of attempts to recover an On-Demand Scan task after Kaspersky Embedded Systems Security for Windows returns an error. The entry field is available if the **Perform task recovery** check box is selected.
Do not start scheduled scan tasks	This check box enables or disables the start of a scheduled scan task after the protected device switches to a UPS source until the standard power supply is restored. If the check box is selected, Kaspersky Embedded Systems Security for Windows does not start scheduled scan tasks after the protected device switches to a UPS source until the standard power supply is restored. If the check box is cleared, Kaspersky Embedded Systems Security for Windows starts scheduled scan tasks regardless of the power supply. The check box is selected by default.
Stop current scan tasks	The check box enables or disables running scan tasks after the protected device switches to a UPS source. If the check box is selected, Kaspersky Embedded Systems Security for Windows pauses running scan tasks after the protected device switches to a UPS source.

	If the check box is cleared, Kaspersky Embedded Systems Security for Windows continues running scan tasks after the protected device switches to a UPS source. The check box is selected by default.
Apply password protection	Set a password to protect access to Kaspersky Embedded Systems Security for Windows functions.

Configuring connection settings in Web Plug-in

The configured connection settings are used to connect Kaspersky Embedded Systems Security for Windows to update and activation servers and during integration of applications with KSN services.

To configure the connection settings take the following steps:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.
2. Click the policy name you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.
4. Select the **Application settings** section.
5. Click the **Settings** button in the **Scalability, interface and scan settings** subsection.
6. Configure the settings described in the table below.

Connection settings

Setting	Description
Do not use proxy server	If this option is selected, Kaspersky Embedded Systems Security for Windows connects to KSN services directly, without using any proxy server.
Use specified proxy server settings	If this option is selected, Kaspersky Embedded Systems Security for Windows connects to KSN using proxy server settings specified manually.
Do not use proxy server for local addresses	This check box enables or disables the use of a proxy server when accessing devices located in the same network as the protected device with Kaspersky Embedded Systems Security for Windows installed. If this check box is selected, devices are accessed directly from the network that hosts the protected device with Kaspersky Embedded Systems Security for Windows installed. No proxy server is used. If the check box is cleared, a proxy server is used to connect to local devices. The check box is selected by default.
Proxy server authentication settings	Specify the authentication settings
Do not use authentication	Authentication is not performed. The mode is selected by default.
Use NTLM authentication	Authentication is performed using the NTLM network authentication protocol developed by Microsoft.
Use NTLM	Authentication is performed with a user name and password using the NTLM

authentication with user name and password	network authentication protocol developed by Microsoft.
Apply user name and password	Authentication is performed using the user name and password.

Configuring scheduled start of local system tasks

You can use policies to allow or block the start of the local system On-Demand Scan task and the Update task. This is done according to the schedule configured locally on each protected device in the administration group:

- If the scheduled start of a specific type of local system task is prohibited by a policy, these tasks will not be performed on the protected device according to the schedule. You can start local system tasks manually.
- If the scheduled start of a specific type of local system task is allowed by a policy, these tasks will be performed in accordance with the scheduled parameters configured locally for this task.

By default, starting of local system tasks is prohibited by policy.

We recommend that you do not allow local system tasks to start if updates or on-demand scans are administered by Kaspersky Security Center group tasks.

If you do not use group update or on-demand scan tasks, allow local system tasks to be started in the policy: Kaspersky Embedded Systems Security for Windows will perform application database and module updates, and start all local system on-demand scan tasks in accordance with the default schedule.

You can use policies to allow or block the scheduled start of the following local system tasks:

- On-Demand Scan tasks: Critical Areas Scan, Quarantine Scan, Scan at Operating System Startup, Application Integrity Control, Baseline File Integrity Monitor.
- Update tasks: Database Update, Software Modules Update, Copying Updates.

If the protected device is excluded from the administration group, the local system tasks schedule will be enabled automatically.

To allow or block the scheduled start of Kaspersky Embedded Systems Security for Windows local system tasks in a policy:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.
2. Click the policy name you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.
4. Select the **Application settings** section.
5. Click the **Settings** button in the **Run local system tasks** subsection.
6. Configure the settings described in the table below.

Scheduled launch of local system tasks settings

Setting	Description
Allow on-demand scan tasks launch	Select or clear the check box to allow or disallow the scheduled launch of on-demand scan tasks.
Allow update tasks and Copying Update task launch	Select or clear the check box to allow or disallow the scheduled launch of update tasks and Copying Update task.

Configuring Quarantine and Backup settings in Web Plug-in

To configure general Quarantine and Backup settings in Kaspersky Security Center:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.
2. Click the policy name you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.
4. Select the **Supplementary** section.
5. Click the **Settings** button in the **Storages** subsection.
6. Configure the settings described in the table below.

Quarantine and Backup settings

Setting	Description
Backup folder	Specify the backup folder.
Maximum Backup size (MB)	Set the maximum Backup size.
Threshold value for space available (MB)	Specify the minimum value of free space in the Backup folder.
Target folder for restoring objects	Specify a folder for restored objects.
Quarantine folder	Specify the backup folder.
Maximum Quarantine size (MB)	Set the maximum Backup size.
Threshold value for space available (MB)	Specify the minimum value of free space in the Backup folder.
Target folder for restoring objects	Specify a folder for restored objects.
Network session blocking term	Specify the number of days, hours and minutes after which blocked network sessions regain access to network file resources.

Creating and configuring policies

This section provides information on using Kaspersky Security Center policies for managing Kaspersky Embedded Systems Security for Windows on several protected devices.

Global Kaspersky Security Center policies can be created for managing protection on several devices where Kaspersky Embedded Systems Security for Windows is installed.

A policy enforces the specified Kaspersky Embedded Systems Security for Windows settings, functions and tasks on all protected devices for one administration group.

Several policies for one administration group can be created and enforced in turns. The policy currently active for a group has *active* status in the Administration Console.

Information on policy enforcement is logged in the Kaspersky Embedded Systems Security for Windows system audit log. This information can be viewed in the Application Console in the **System audit log** node.

Kaspersky Security Center offers one way to apply policies on protected devices: *Prohibit changing the settings*. After a policy has been applied, Kaspersky Embedded Systems Security for Windows uses the settings for which you have selected the icon in the policy properties on protected devices. In this case, the selected settings are used instead of the settings in effect before the policy was applied. Kaspersky Embedded Systems Security for Windows does not apply the active policy settings for which the icon is selected in the policy properties.

If a policy is active, the values of settings marked with the icon in the policy are displayed in the Application Console but cannot be edited. The values of other settings (marked with the icon in the policy) can be edited in the Application Console.

The settings configured in the active policy and marked with the icon also block changes in Kaspersky Security Center for an individual protected device in the **Properties: <Protected device name>** window.

Settings that are specified and sent to the protected device using an active policy are saved in the local task settings after the active policy is disabled.

If a policy defines settings for any Real-Time Computer Protection task that is currently running, the settings defined by the policy will change immediately after the policy is applied. If the task is not running, the settings are applied when it starts.

Creating a policy

To create a policy:

1. In the main window of the Web Console, select **Devices** → **Policies & profiles**.
2. Click the **Add** button.
3. The **New policy** window opens.
4. In the **Select application** section, select Kaspersky Embedded Systems Security for Windows and click **Next**.
5. On the **General** tab, you can perform the following actions:
   - Change the policy name.

The policy name cannot contain the following symbols: " * < : > ? \ | .

- Select the policy status:
  - **Active**. After the next synchronization, the policy will be used as the active policy on the computer.
  - **Inactive**. Backup policy. If necessary, an inactive policy can be switched to active status.
  - **Out-of-office**. The policy is activated when a computer leaves the organization network perimeter.
- Configure the inheritance of settings:
  - **Inherit settings from parent policy**. If this toggle button is switched on, the policy setting values are inherited from the top-level policy. Policy settings cannot be edited if is set for the parent policy.
  - **Force inheritance of settings in child policies**. If the toggle button is on, the values of the policy settings are propagated to the child policies. In the child policy settings the **Inherit settings from parent policy** check box is automatically selected. Child policy settings are inherited from the parent policy, except for the settings marked with . Child policy settings cannot be edited if is set for the parent policy.

6. On the **Application settings** tab, configure the policy settings as required.

7. Click the **Save** button.

The created policy appears in the list of policies on the **Policies & profiles** tab of the selected administration group. In the **<Policy name>** window, you can configure other settings, tasks and functions of Kaspersky Embedded Systems Security for Windows.

After a new policy is created, a set of allowing rules is created to prevent applications from being blocked, ensuring their uninterrupted operation. You can view the default rules in the task settings. See below for details and limitations.

By default, Kaspersky Embedded Systems Security for Windows creates a set of rules for inbound network traffic when creating a new policy:

- Two allowing rules for the process of sharing the Windows desktop using Kaspersky Security Center Network Agent, which is located in the %Program Files% and %Program Files (x86)% folders. Status: enabled. Allowed external addresses: all. Protocols: TCP and UDP, one rule per protocol.
- Two allowing rules for local port 15000. State: enabled. Allowed external addresses: all. Protocols: TCP and UDP, one rule per protocol.

By default, Kaspersky Embedded Systems Security for Windows creates a set of outgoing network traffic rules when creating a new policy:

- Two allowing rules for the Kaspersky Embedded Systems Security for Windows service, which is located in the %Program Files% and %Program Files (x86)% folders. Status: enabled. Allowed external addresses: all. Protocols: TCP and UDP, one rule per protocol.
- Two allowing rules for the worker process of Kaspersky Embedded Systems Security for Windows, which is located in the %Program Files% and %Program Files (x86)% folders. Status: enabled. Allowed external addresses: all. Protocols: TCP and UDP, one rule per protocol.
- Two allowing rules for local port 13000. State: enabled. Allowed external addresses: all. Protocols: TCP and UDP, one rule per protocol.

Kaspersky Embedded Systems Security for Windows policy settings sections

General

In the **General** section, you can configure the following policy settings:

- Indicate the policy status.
- Configure the inheritance settings for parent and child policies.

Event configuration

In the **Event configuration** section, you can configure settings for the following event categories:

- *Critical event*
- *Functional failure*
- *Warning*
- *Info*

You can use the **Properties** button to configure the following settings for the selected events:

- Indicate the storage location and retention period for information about logged events.
- Indicate the notification method for logged events.

Application settings

Settings of the Application Settings section

Section	Options
Scalability, interface and scan settings	In the **Scalability, interface and scan settings** subsection, you can click the **Settings** button to configure the following settings: • Choose whether to configure scalability settings automatically or manually. • Configure the application icon display settings.
Security and reliability	In the **Security and reliability** subsection, you can click the **Settings** button to configure the following settings: • Configure the task start settings. • Specify how the application should behave when the protected device is running on UPS power. • Enable or disable password-protection of application functions.
Connections	In the **Connections** subsection, you can use the **Settings** button to configure the following proxy server settings for connecting with update servers, activation servers, and KSN: • Configure the proxy server settings. • Specify the proxy server authentication settings.
Run local system tasks	In the **Run local system tasks** subsection, you can use the **Settings** button to allow or block the start of the following local system tasks according to a schedule configured on protected devices: • On-Demand Scan task. • Update tasks and Copying Update task.

Supplementary

Settings of the Supplementary section

Section	Options
Trusted Zone	In the **Settings** subsection, you can click the **Trusted Zone** button to configure the following Trusted Zone settings: • Create a list of Trusted Zone exclusions. • Enable or disable scanning of file backup operations.

	• Create a list of trusted processes.
Removable Drives Scan	In the **Removable Drives Scan** subsection, you can use the **Settings** button to configure scan settings for removable drives.
User access permissions for application management	In the **User access permissions for application management** subsection, you can configure user rights and user group rights to manage Kaspersky Embedded Systems Security for Windows.
User access permissions for Kaspersky Security Service management	In the **User access permissions for Kaspersky Security Service management** subsection, you can configure user rights and user group rights to manage the Kaspersky Security Service.
Storages	In the **Storages** subsection, click the **Settings** button to configure the following Quarantine, Backup and Blocked Hosts settings: • Specify the path to the folder where you want to place Quarantine or Backup objects. • Configure the maximum size of Backup and Quarantine and also specify the available space threshold. • Specify the path to the folder where you want to place objects restored from Quarantine or Backup. • Configure transmission of information about Quarantine and Backup objects to Administration Server. • Configure how long hosts are blocked.

Real-time computer protection

Settings of the Real-Time Server Protection section

Section	Options
Real-Time File Protection	In the **Real-Time File Protection** subsection, you can click the **Settings** button to configure the following settings: • Indicate the protection mode. • Configure use of the Heuristic Analyzer. • Configure application of the trusted zone. • Indicate the protection scope. • Set the security level for the selected protection scope: you can select a predefined security level or configure the security settings manually. • Configure the task start settings.
KSN Usage	In the **KSN Usage** subsection, you can click the **Settings** button to configure the following task settings: • Indicate the actions to perform on KSN untrusted objects. • Configure data transfer and usage of Kaspersky Security Center as a KSN proxy server.

Exploit Prevention	In the **Exploit Prevention** subsection, you can click the **Settings** button to configure the following task settings: • Select the process memory protection mode. • Indicate actions to reduce exploit risks. • Add to and edit the list of protected processes.

Local activity control

Settings of the Local Activity Control section

Section	Options
Applications Launch Control	In the **Applications Launch Control** subsection, you can use the **Settings** button to configure the following task settings: • Select the task operating mode. • Configure settings for controlling subsequent application launches. • Indicate the scope of the Applications Launch Control rules. • Configure use of KSN. • Configure the task start settings.
Device control	In the **Device control** subsection, you can click the **Settings** button to configure the following task settings: • Select the task operating mode. • Configure the task start settings.

Network activity control

Settings of the Network activity control section

Section	Options
Firewall Management	In the **Firewall Management** subsection, you can click the **Settings** button to configure the following task settings: • Configure firewall rules. • Configure the task start settings.

System Inspection

Settings of the System Inspection section

Section	Options
File Integrity Monitor	In the **File Integrity Monitor** subsection, you can configure control over changes in files that can signify a security breach on a protected device.
Log Inspection	In the **Log Inspection** subsection, you can configure monitoring of the integrity of the protected device based on the results of an analysis of the Windows Event Log.

Logs and notifications

Settings of the Logs and Notifications section

Section	Options
Task logs	In the **Task logs** subsection, you can click the **Settings** button to configure the following settings: • Specify the importance level of the logged events for the selected software components. • Specify the task log storage settings. • Specify the SIEM integration with Kaspersky Security Center settings.
Event notifications	In the **Event notifications** subsection, you can click the **Settings** button to configure the following settings: • Specify the user notification settings for the *Object detected*, *Untrusted mass storage detected and restricted*, and *Host listed as untrusted* events. • Specify the administrator notification settings for any event selected in the event list in the **Notification settings** section.
Interaction with Administration Server	In the **Interaction with Administration Server** subsection, you can click the **Settings** button to select the types of objects that Kaspersky Embedded Systems Security for Windows will report to the Administration Server.

Revision history

In the **Revision history** section, you can manage revisions: compare with the current revision or other policy, add descriptions of revisions, save revisions to a file or perform a rollback.

Creating and configuring tasks using Kaspersky Security Center

This section contains information about Kaspersky Embedded Systems Security for Windows tasks, and how to create them, configure task settings, and start and stop them.

About task creation in Web Plug-in

You can create group tasks for administration groups and sets of protected devices. The following types of tasks can be created:

- Activation of Application
- Copying Updates
- Database Update
- Software Modules Update
- Rollback of Database Update
- On-Demand Scan
- Application Integrity Control
- Baseline File Integrity Monitor
- Rule Generator for Applications Launch Control
- Rule Generator for Device Control

You can create local and group tasks in the following ways:

- For one protected device: in the **Properties <Protected device name>** window in the **Tasks** section.
- For an administration group: in the details pane of the node of the selected group of protected devices on the **Tasks** tab.
- For a set of protected devices: in the details pane of the **Device selections** node.

You can use policies to disable schedules for update and On-Demand Scan local system tasks on all protected devices in the same administration group.

General information on tasks in Kaspersky Security Center is provided in the *Kaspersky Security Center Help*.

Creating a task in Web Plug-in

To create a new task in the Kaspersky Security Center Administration Console:

1. Start the task wizard in one of the following ways:
   - To create a local task:
     a. In the main window of the Web Console, select **Devices** → **Managed devices**.
     b. Click the protected device name.
     c. In the **<Device name>** window that opens, select the **Tasks** tab.
     d. Click the **Add** button.

- To create a group task:

  a. In the main window of the Web Console, select **Devices** → **Tasks**.

  b. Click the **Add** button.

- To create a task for a custom set of protected devices:

  a. In the main window of the Web Console, select **Devices** → **Device selections**.

  b. Select the selection for which you want to create a task.

  c. Click the **Start** button.

  d. In the **Selection results** window, select the devices for which you want to create a task.

  e. Click the **New task** button.

The task wizard window opens.

2. In the **Application** drop-down list, select **Kaspersky Embedded Systems Security for Windows**.

3. In the **Task type** drop-down list, select the type of the task to be created.

   If you selected any task type except Rollback of Database Update, Application Integrity Control or Activation of the Application, the settings window opens.

4. Depending on the selected task type, do one of the following:

   - Create an On-Demand Scan task.

   - To create an update task, configure task settings based on your requirements:

     a. Select an update source in the **Database update source** section.

     b. In the **Connection settings** window, configure the proxy server settings.

   - After creating a Software Modules Update task, configure the required application module update settings in the **Software Modules Update** window:

     a. Select whether to copy and install critical software module updates, or only to check for their availability without installation.

     b. If **Copy and install critical software modules updates** is selected: a protected device restart may be required to apply the installed software modules. If you wish Kaspersky Embedded Systems Security for Windows to restart the protected device automatically upon task completion, select the **Allow operating system restart** check box.

     c. To obtain information about Kaspersky Embedded Systems Security for Windows module upgrades, select **Receive information about available scheduled software modules updates**.

     Kaspersky does not publish planned update packages on the update servers for automatic installation; these can be downloaded manually from the Kaspersky website. An administrator notification about the **New scheduled software modules update is available** event can be configured. This will contain the URL of our website from which scheduled updates can be downloaded.

   - To create the Copying Updates task, specify the set of updates and the destination folder in the **Copying Updates** window.

- To create the Activation of the Application task:

  a. In the **List of keys in Kaspersky Security Center storage** window, specify the key file that you want to use to activate the application.

  b. Select the **Use as additional key** check box if you want to create a task for renewing the license.

- Create and configure the Rule Generator for Applications Launch Control task.

- Create and configure Rule Generator for Device Control task.

5. Click the **Next** button.

6. If the task is being created for a set of protected devices, select the network (or group) of protected devices on which this task will be executed.

7. Click the **Next** button.

8. In the **Finishing creation** window, select the **Open task details when creation is complete** check box if you want to configure task settings.

9. Click the **Finish** button.

The task created is displayed in the **Tasks** list.

Configuring group tasks in Web Plug-in

To configure a group task for multiple protected devices:

1. In the main window of the Web Console, select **Devices** → **Tasks**.

2. Click the task name in the list of Kaspersky Security Center tasks.

   The **<Task name>** window opens.

3. Depending on the type of configured task, do one of the following:

   - To configure an On-Demand Scan task:

     a. In the **Scan scope** section, configure a scan scope.

     b. In the **Options** section, configure the task priority level and integration with other software components.

   - To configure an update task, adjust the task settings based on your requirements:

     a. In the **Update sources** section, configure update source and proxy server settings.

     b. In the **Optimization** section, configure disk subsystem optimization.

   - To configure the Software Modules Update task, in the **Advanced settings** section, choose an action to perform: copy and install critical updates of software modules or only check for them.

   - To configure the Copying Updates task, specify the set of updates and the destination folder in the **Copying updates settings** section.

- To configure the Activation of the Application task, apply the key file that you want to use to activate the application. Select the **Use as additional key** check box if you want to add an activation code or key file for renewing the license.

- To configure the automatic generation of allowing rules for Device Control, specify the settings that will be used to create the list of allowing rules.

4. Configure the task schedule in the **Schedule** section (you can configure a schedule for all task types except Rollback of Database Update).

5. On the **Settings** tab in the **Account** section, specify the account whose rights will be used to run the task. For detailed information on configuring settings in this section, see *Kaspersky Security Center Help*.

6. Click the **Save** button.

The newly configured group task settings are saved.

Configuring Activation of the Application task in Web Plug-in

To configure an Activation of the Application task:

1. In the main window of the Web Console, select **Devices** → **Tasks**.

2. Click the task name in the list of Kaspersky Security Center tasks.

   The **<Task name>** window opens.

3. In the **Common** section, specify the key file that you want to use to activate the application. Select the **Use as additional key** check box if you want to add a key to renew the license.

4. Configure the task schedule in the **Schedule** section.

5. In the **<Task name>** window, click **OK**.

Configuring Update tasks in Web Plug-in

To configure the Copying Updates, Database Update, or Software Modules Update tasks:

1. In the main window of the Web Console, select **Devices** → **Tasks**.

2. Click the task name in the list of Kaspersky Security Center tasks.

   The **<Task name>** window opens.

3. In the **Update sources** section, configure update source settings:

   - In the **Database update source** section, specify Kaspersky Security Center Administration Server or Kaspersky update servers as an application update source. You can also create a customized list of update sources: by adding custom HTTP and FTP servers or network folders manually, and setting them as update sources.

     You can specify the usage of Kaspersky update servers, if manually customized servers are not available.

To use an SMB-shared folder as an update source, you need to specify a user account to start a task.

When configuring an update task via the Cloud Console, only **Distribution points** and **Kaspersky update servers** settings are available to specify the update source.

- In the **Connection settings** section, configure the use of a proxy server for connecting to Kaspersky update servers and other servers.

4. In the **Optimization** section for the Database Update task, you can configure the feature that reduces the workload on the disk subsystem:
   - **Disk I/O usage optimization**
   - **RAM used for optimization (400 - 9999 MB)**
5. Configure the task schedule in the **Schedule** section (you can configure a schedule for all task types except Rollback of Database Update).
6. In the **<Task name>** window, click **OK**.

Configuring crash diagnostics settings in Web Plug-in

If a problem occurs in the operation of Kaspersky Embedded Systems Security for Windows (for example, the application crashes), you can troubleshoot it. To do this, you can enable the creation of trace files and a dump file for the Kaspersky Embedded Systems Security for Windows process and send these files for analysis to Technical Support.

Kaspersky Embedded Systems Security for Windows does not send any trace or dump files automatically. Diagnostic data can only be sent by a user who has the required permissions.

Kaspersky Embedded Systems Security for Windows writes information to trace files and the dump file in unencrypted form. The folder where files are saved is selected by the user and managed by the operating system configuration and Kaspersky Embedded Systems Security for Windows settings. You can configure access permissions and allow only required users to access logs, trace files and dump files.

To configure crash diagnostics settings in Kaspersky Security Center:

1. In the Kaspersky Security Center Administration Console, open the **Application settings** window.
2. Open the **Malfunction diagnosis** section.
3. To log debug information to a file, in the **Troubleshooting settings** section, select the **Enable tracing** check box.
4. In the **Trace files folder** field, specify the absolute path to the local folder where Kaspersky Embedded Systems Security for Windows will save trace files.

   The folder must be created in advance and be writable by the SYSTEM account. You cannot specify a network folder, drive, or environment variables.

5. Configure the level of detail of debug information.

6. Specify the **Maximum size of trace files (MB)**.

   Available values: from 1 to 4095 MB. By default, the maximum size of trace files is 50 MB.

7. To delete the oldest trace files when the maximum number of files is reached, select the **Remove older trace files** check box.

8. Specify the **Maximum number of files for one trace log**.

   Available values: from 1 to 999. By default, the maximum number of files is 5. The field is available if the **Remove older trace files** check box is selected.

9. If you want the application to create a dump file, select the **Create dump file** check box.

10. In the **Dump files folder** field, specify the absolute path to the local folder where Kaspersky Embedded Systems Security for Windows will save dump files.

    The folder must be created in advance and be writable by the SYSTEM account. You cannot specify a network folder, drive, or environment variables.

11. Click the **OK** button.

The configured application settings are applied on the protected device.

Managing task schedules

You can configure the start schedule for Kaspersky Embedded Systems Security for Windows tasks, and configure settings for running tasks on a schedule.

Scheduling tasks

You can schedule local system and custom tasks in the Application Console. You cannot schedule group tasks in the Application Console.

To schedule group tasks using the Web Plug-in:

1. In the main window of the Web Console, select **Devices** → **Tasks**.

2. Click the task name in the list of Kaspersky Security Center tasks.

   The **<Task name>** window opens.

3. Select the **Application settings** section.

4. In the **Schedule** section, select the **Run by schedule** check box.

   Fields with schedule settings for the On-Demand Scan and Update tasks are unavailable if scheduling of these tasks is blocked by a Kaspersky Security Center policy.

5. Configure schedule settings in accordance with your requirements. To do this, perform the following actions:

a. in the **Frequency** list, select one of the following values:

- **Hourly**, if you want the task to run at intervals of a specified number of hours; specify the number of hours in the **Every <number> hour(s)** field.
- **Daily**, if you want the task to run at intervals of a specified number of days; specify the number of days in the **Every <number> day(s)** field.
- **Weekly**, if you want the task to run at intervals of a specified number of weeks; specify the number of weeks in the **Every <number> week(s)** field. Specify the days of the week on which the task will be started (by default tasks run on Mondays).
- **At application launch**, if you want the task to run every time Kaspersky Embedded Systems Security for Windows starts.
- **After application database update**, if you want the task to run after every update of the application databases.

b. Specify the time for the first task start in the **Start time** field.

c. In the **Start date** field, specify the date when the schedule starts.

6. In the **Task stop settings** section:

a. Select the **Duration** check box and, in the fields to the right, enter the maximum number of hours and minutes of task execution.

b. Select the **Pause task** check box and, in the fields to the right, enter the start and end values of a time interval under 24 hours during which task execution will be paused.

7. In the **Advanced schedule settings** block:

a. Select the **Cancel schedule** check box and specify the date from which the schedule will cease to apply.

b. Select the **Run skipped tasks** check box to enable the start of skipped tasks.

c. Select the **Randomize the task start time within the interval** check box and specify a value in minutes.

8. Click the **Save** button to save the task start settings.

Enabling and disabling scheduled tasks

You can enable and disable scheduled tasks either before or after configuring the schedule settings.

To enable or disable the task start schedule:

1. In the main window of the Web Console, select **Devices** → **Tasks**.
2. Click the task name in the list of Kaspersky Security Center tasks.

   The **<Task name>** window opens.
3. Select the **Application settings** section.

4. Select the **Schedule** section.

5. Do one of the following:

   - Select the **Run by schedule** check box if you want to enable scheduled task start.
   - Clear the **Run by schedule** check box if you want to disable scheduled task start.

     The configured task start schedule settings are not deleted and will be applied at the next time you enable a scheduled task start.

6. Click the **Save** button.

The configured task start schedule settings are saved.

Reports in Kaspersky Security Center

Reports in Kaspersky Security Center contain information about the status of managed devices. Reports are based on information stored on Administration Server.

Starting from Kaspersky Security Center 11, the following types of reports are available for Kaspersky Embedded Systems Security for Windows:

- Report on the status of application components
- Report on prohibited applications
- Report on prohibited applications in test mode

See *Kaspersky Security Center Help* for detailed information about all Kaspersky Security Center reports and how to configure them.

Report on the status of Kaspersky Embedded Systems Security for Windows components

You can monitor the protection status of all network devices and get a structured overview of the set of components on each device.

The report displays one of the following states for each component: *Running*, *Paused*, *Stopped*, *Malfunction*, *Not installed*, *Starting*.

Not Installed status refers to the component, not the application itself. If the application is not installed, the Kaspersky Security Center Web Console assigns the N/A (Not available) status.

You can create component selections and use filtering to display network devices with a specified set of components and state.

See *Kaspersky Security Center Help* for detailed information about creating and using selections.

To review the status of components in the application settings:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the protected device name.
3. On the **General** tab, select the **Components** section.
4. Review the status table.

> Information about Exploit Prevention component status is not available in this table.

To review a Kaspersky Security Center Web Console standard report:

1. Select **Monitoring and Reporting** → **Reports**.
2. Select the **Report on the status of application components** list item and click the **Show report** button.

   A report is generated.
3. Review the following report details:

   - A graphical diagram.
   - A summary table of components and aggregated numbers of network devices where each of the components is installed, and groups they belong to.
   - A detailed table specifying the component status, version, device and group.

Reports on prohibited applications in active and test modes

Based on the results of the Applications Launch Control task, two types of reports can be generated: a report on prohibited applications (if the task is started in Active mode) and a report on prohibited applications in test mode (if the task is started in Statistics only mode). These reports display information about blocked applications on the protected devices of the network. Each report is generated for all administration groups and accumulates data from all the Kaspersky applications installed on the protected devices.

To review a report on prohibited applications in Statistics only mode:

1. Start the Applications Launch Control task in Statistics only mode.
2. Select **Monitoring and Reporting** → **Reports**.
3. Select the **Report on prohibited applications in test mode** list item and click the **Show report** button.

   A report is generated.
4. Review the following report details:

   - A graphical diagram that displays the top 10 applications with the largest number of blocked starts.
   - A summary table of application blocks, specifying the executable file name, reason, time of blocking, and number of devices where the blocking occurred.
   - A detailed table specifying data about the device, file path and criteria for blocking.

To review a report on prohibited applications in Active mode:

1. Start the Applications Launch Control task in Active mode.
2. Select **Monitoring and Reporting → Reports**.
3. Select the **Report on prohibited applications in test mode** list item and click the **Show report** button.
   A report is generated.

This report consists of the same data about blocks as the report on prohibited applications in test mode.

Compact Diagnostic Interface

This section describes how to use the Compact Diagnostic Interface for reviewing protected device status or current activity, and how to configure writing of dump and trace files.

About the Compact Diagnostic Interface

The Compact Diagnostic Interface component (also referred to as the "CDI") is installed and uninstalled along with the System Tray Icon component independently from the Application Console, and can be used when the Application Console is not installed on the protected device. The Compact Diagnostic Interface is started from the System Tray Icon or by running kavfsmui.exe from the application folder on the protected device.

In the Compact Diagnostic Interface, you can do the following:

- Review information about the general application status.
- Review security incidents that have occurred.
- Review current activity on the protected device.
- Start or stop writing dump and trace files.
- Open the Application Console.
- Open the **About the application** window with the list of installed updates and available patches.

The Compact Diagnostic Interface is available even if access to Kaspersky Embedded Systems Security for Windows functions is password-protected. No password is required.

> The Compact Diagnostic Interface component cannot be configured via Kaspersky Security Center.

Reviewing the Kaspersky Embedded Systems Security for Windows status via the Compact Diagnostic Interface

To open the Compact Diagnostic Interface, perform the following actions:

1. Right-click the Kaspersky Embedded Systems Security for Windows System Tray Icon in the toolbar notification area.
2. Select the **Open Compact Diagnostic Interface** option.

   The **Compact diagnostic interface** opens.

Review the current status of the key, Real-Time Computer Protection tasks, and Update tasks on the **Protection status** tab. Different colors are used to notify the user about the protection status (see the table below).

Protection status in the Compact Diagnostic Interface

Section	Status

Real-time protection status	The panel is *green* for either of the following scenarios (if any of the conditions are met):
	• Recommended configuration:
	  • The Real-Time File Protection task is started with the default settings.
	  • The Applications Launch Control task is started in **Active** mode with the default settings.
	• Acceptable configuration:
	  • The Real-Time File Protection task is configured by the user.
	  • Applications Launch Control task settings are modified.

	The panel is *yellow* if one or more of the following conditions are met: • The Real-Time File Protection task is paused (by the user or schedule). • The Applications Launch Control task is started in **Statistics only** mode. • Exploit Prevention and the Applications Launch Control task are started in **Statistics only** mode.
	The panel is *red* if both of the following conditions are met: • The Real-Time File Protection component is not installed or the task is stopped or paused. • The Applications Launch Control component is not installed or the task is started in **Statistics only** mode.
Licensing	The panel is *green* if the current license is valid.
	A *yellow* panel signifies that one of the following events has occurred: • *Checking the license status*. • *The license will expire in 14 days and no additional key or activation code has been added.* • *The added key has been added to the denylist and is about to be blocked.*
	A *red* panel signifies that one of the following events has occurred: • *Application not activated* • *License has expired* • *End User License Agreement has been violated* • *License key has been added to the denylist of keys*
Update	The panel is *green* when Application databases are up-to-date.
	The panel is *yellow* when Application databases are out of date.

	The panel is *red* when Application databases are extremely out of date.

Reviewing security event statistics

The **Statistics** tab displays all security events. Each protection task statistic is displayed in a separate block specifying the number of incidents and the date, and time when the last incident occurred. When an incident is logged, the block color changes to red.

To review the statistics:

1. Right-click the Kaspersky Embedded Systems Security for Windows System Tray Icon in the toolbar notification area.
2. Select the **Open Compact Diagnostic Interface** option.

   The **Compact diagnostic interface** opens.
3. Open the **Statistics** tab.
4. Review the security incidents for the protection tasks.

Reviewing current application activity

On this tab, you can review the status of current tasks and application processes, and promptly get notifications about critical events that occur.

Different colors are used to indicate the application activity status:

- In the **Tasks** section:
  - *Green*. There are no conditions that would require yellow or red.
  - *Yellow*. Critical areas have not been scanned for a long time.
  - *Red*. At least one of the following conditions is true:
    - No tasks are started and a start schedule is not set up for any of the tasks.
    - Application launch errors are logged as critical events.
- In the **Kaspersky Security Network** section:
  - *Green*. The KSN Usage task is started.
  - *Yellow*. The KSN Statement is accepted, but the task is not started.

To review the current application activity on the protected device:

1. Right-click the Kaspersky Embedded Systems Security for Windows System Tray Icon in the toolbar notification area.
2. Select the **Open Compact Diagnostic Interface** option.

The **Compact diagnostic interface** opens.

3. Open the **Current application activity** tab.
4. Review the following information in the **Tasks** section:
   - **Critical areas not scanned for a long time**.

     This field is displayed only if the application returns a corresponding warning about critical area scans.

   - **Running now**
   - **Execution failed**
   - **Next start defined by a schedule**
5. Review the following information in the **Kaspersky Security Network** section:
   - **KSN is on. File reputation services are enabled** or **Protection is off**.
   - **KSN is on. File reputation services are enabled, application statistics is being sent to KSN.**

     The application sends information about malware, including fraudulent software, detected during execution of the Real-Time File Protection task and the On-Demand Scan tasks, as well as debugging information about errors during scanning.

     The field is displayed if the **Send Kaspersky Security Network statistics** check box is selected in the KSN Usage task settings.
6. Review the following information in the **Integration with Kaspersky Security Center** section:
   - **Local management is allowed**.
   - **Policy is applied: <Administration Server name>**.

Configuring writing of dump and trace files

You can configure the writing of dump and trace files in the Compact Diagnostic Interface.

You can also configure malfunction diagnostics via the Application Console.

To start writing dump and trace files, perform the following actions:

1. Right-click the Kaspersky Embedded Systems Security for Windows System Tray Icon in the toolbar notification area.
2. Select the **Open Compact Diagnostic Interface** option.

   The **Compact diagnostic interface** opens.
3. Open the **Troubleshooting** tab.

4. Change the following trace settings if necessary:

    a. Select the **Write debug information to trace file** check box.

    b. Click the **Browse** button to specify the folder where Kaspersky Embedded Systems Security for Windows will save trace files.

    Tracing will be enabled for all components with the default settings using the *Debug* level of detail and the default maximum log size of 50 MB.

5. Change the following dump-file settings if necessary:

    a. Select the **Create dump file on malfunction in this folder** check box.

    b. Click the **Browse** button to specify the folder where Kaspersky Embedded Systems Security for Windows will save the dump file.

6. Click the **Apply** button.

    The new configuration will be applied.

Kaspersky Embedded Systems Security for Windows database and software modules update

This section provides information about Kaspersky Embedded Systems Security for Windows databases and software module update tasks, copying updates and rolling back database updates of Kaspersky Embedded Systems Security for Windows, as well as instructions on how to configure database and software module update tasks.

Updates functionality (including providing anti-virus signature updates and codebase updates), as well as KSN functionality may not be available in the program in the U.S.

About Update tasks

Kaspersky Embedded Systems Security for Windows offers six update tasks: Application Database Update, Software Modules Update, Copying Updates, Rollback, Secure Application Database Copy, and Secure Application Database Update.

By default, Kaspersky Embedded Systems Security for Windows connects to the update source every hour. You can configure all Update tasks, except for the Rollback of Database Update task. When task settings are modified, Kaspersky Embedded Systems Security for Windows will apply the new values at the next task start.

You are not allowed to pause and resume Update tasks.

Database Update

By default, Kaspersky Embedded Systems Security for Windows copies databases from the update source to the device and immediately starts using them in the running Real-Time Computer Protection task. The On-Demand Scan tasks start using the updated database at the next start.

By default, Kaspersky Embedded Systems Security for Windows runs the Database Update task every hour.

Software Modules Update

By default, Kaspersky Embedded Systems Security for Windows checks whether software module updates are available on the update source. In order to start using installed software modules, a protected device restart and / or a restart of Kaspersky Embedded Systems Security for Windows is required.

By default, Kaspersky Embedded Systems Security for Windows runs the Software Modules Update task on a weekly basis on Fridays at 4:00 PM (according to the regional time settings of the protected device). During task execution, the application checks for availability of important and scheduled updates of Kaspersky Embedded Systems Security for Windows modules without distributing them.

Copying Updates

By default, during task execution, Kaspersky Embedded Systems Security for Windows downloads Database Update files and saves them to the specified network or local folder without applying them.

The Copying Updates task is disabled by default.

Rollback of Database Update

During task execution, Kaspersky Embedded Systems Security for Windows returns to using databases from previously installed updates.

The Rollback of Database Update task is disabled by default.

Secure Application Database Copy

While the task runs, the Kaspersky Embedded Systems Security for Windows task instance installed on a device that has access to the application databases copies its databases to a secure removable drive protected from reading, copying, and writing by potential attackers.

> Only a Rutoken removable drive can be used as a secure removable drive. The application will not recognize any other types of secure removable drives.

The task can only be started manually via the local Kaspersky Embedded Systems Security for Windows Console.

Secure Application Database Update

This task is necessary to update the application databases using a secure removable drive protected from reading, copying, and writing by potential attackers, in a closed corporate network and on devices that do not have access to the application databases.

Kaspersky Embedded Systems Security for Windows copies databases from the secure removable drive onto the device and instantly applies them to the ongoing Real-Time Computer Protection task. The On-Demand Scan tasks start using the updated database at the next start.

The task can only be started manually via the local Kaspersky Embedded Systems Security for Windows Console.

About Software Modules Update

Kaspersky can issue update packages for Kaspersky Embedded Systems Security for Windows modules. The update packages can be *urgent* (or *critical*) or planned. Critical update packages repair vulnerabilities and errors; planned packages add new features or enhance existing features.

Urgent (critical) update packages are uploaded to Kaspersky's update servers. Their automatic installation can be configured using the Software Modules Update task. By default, Kaspersky Embedded Systems Security for Windows runs the Software Modules Update task on a weekly basis on Fridays at 4:00 PM (according to the regional time settings of the protected device).

Kaspersky does not publish planned update packages on its update servers for automatic update; these can be downloaded from the Kaspersky website. The Software Modules Update task can be used to receive information about the release of scheduled Kaspersky Embedded Systems Security for Windows updates.

You can download critical updates from the Internet to each protected device, or you can use a single protected device as an intermediary by copying all updates onto it and then distributing them to the protected devices in the network. In order to copy and save updates without installing them, use the Copying Updates task.

Before updates of modules are installed, Kaspersky Embedded Systems Security for Windows creates backup copies of the previously installed modules. If the software module update process is interrupted or results in an error, Kaspersky Embedded Systems Security for Windows will automatically return to using the previously installed software modules. Software modules can be rolled back manually to the previously installed updates.

During the installation of downloaded updates, the Kaspersky Security Service automatically stops and then restarts.

About Database Update

Kaspersky Embedded Systems Security for Windows databases stored on the protected device quickly become outdated. Kaspersky's virus analysts detect hundreds of new threats daily, create identifying records for them, and include them in application database updates. Database updates are a file or set of files containing records that identify threats discovered during the time since the last update was created. To maintain the required level of device protection, we recommend that database updates are received regularly.

Kaspersky Embedded Systems Security for Windows downloads updates of application databases and modules from Kaspersky's FTP or HTTP update servers, Kaspersky Security Center Administration Server, or other update sources.

Updates can be downloaded to every protected device, either directly, including via the Secure Application Database Update task, or indirectly through a designated intermediary device. Updates will be copied to it, and then distributed to protected devices. If you manage your organization's device security centrally with Kaspersky Security Center, you can leverage the Administration Server to act as a proxy for downloading updates.

Database Update tasks can be started manually or based on a schedule. By default, Kaspersky Embedded Systems Security for Windows runs the Database Update task every hour.

If the update download process is interrupted or results in an error Kaspersky Embedded Systems Security for Windows will automatically switch back to using the databases from the last installed updates. If the Kaspersky Embedded Systems Security for Windows databases become corrupted, they can be manually rolled back to previously installed updates.

By default, if the Kaspersky Embedded Systems Security for Windows databases are not updated within a week from the time that the installed database updates were created, the *Application database is out of date* event occurs. If the databases are not updated for a period of two weeks, the *Application database is extremely out of date* event occurs. Information about the up-to-date status of the databases is displayed in the results pane of the **Kaspersky Embedded Systems Security for Windows** node of the Application Console tree. You can use Kaspersky Embedded Systems Security for Windows general settings to indicate a different number of days before these events occur. You can also configure administrator notifications about these events.

Kaspersky Embedded Systems Security for Windows database and software modules updating schemes

The choice of update source in update tasks depends on the update scheme for databases and software modules used in the organization.

Kaspersky Embedded Systems Security for Windows databases and modules can be updated on the protected devices using the following schemes:

- Download updates directly from the Internet to each protected device (Scheme 1).
- Download updates from the Internet to an intermediate device and distribute updates to protected devices from that device.

Any device with the software listed below installed can serve as an intermediate device:

- Kaspersky Embedded Systems Security for Windows (Scheme 2).
- Kaspersky Security Center Administration Server (Scheme 3).

Updating using an intermediate device not only reduces Internet traffic, but also provides additional network protected device security.

- Download database updates to each protected device via a secure removable drive (scheme 4).

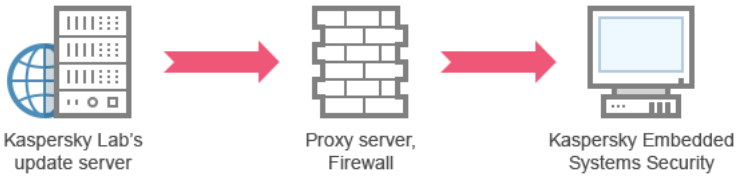
The update schemes listed are described below.

Scheme 1. Updating databases and modules directly from the Internet

To configure Kaspersky Embedded Systems Security for Windows updates directly from the Internet:

on each protected device in the settings of the Database Update task and the Software Modules Update task, specify Kaspersky's update servers as the source of updates.

Other HTTP or FTP servers that have an update folder can be configured as the update source.



Scheme 1: Updating databases and modules directly from the Internet

Scheme 2. Updating databases and modules via one of the protected devices

To configure Kaspersky Embedded Systems Security for Windows updates via one of the protected devices:

1. Copy updates to the selected protected device.
   - Configure the Copying Updates task settings on the selected protected device:
     a. Specify Kaspersky's update server as the update source.
     b. Specify a shared folder to be used as the folder where updates are saved.

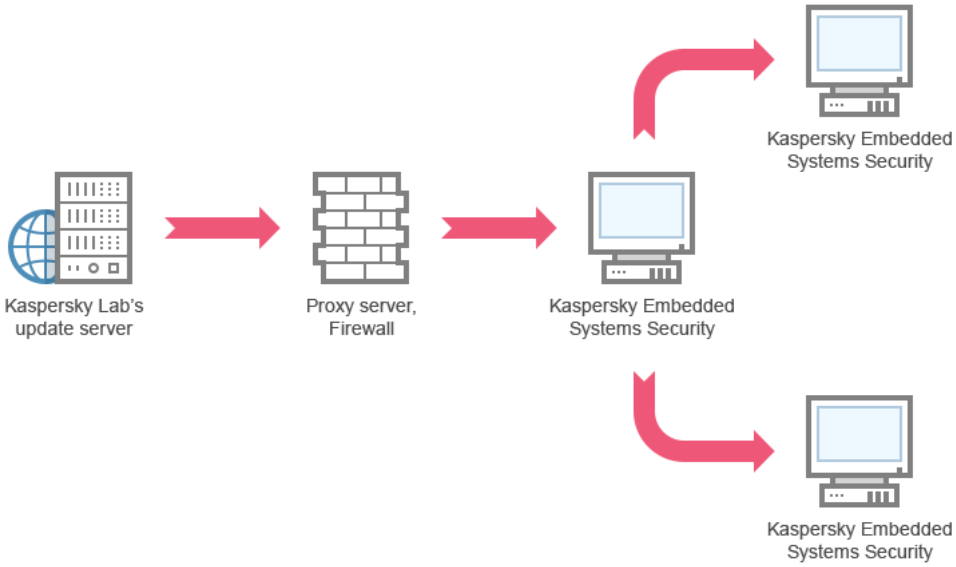
     We recommend to deny access to the shared folder for relaying updates to all user groups on the device with the shared folder, except for the Administrators and SYSTEM groups. We recommend to grant the Administrators group read, view, and run rights, and grant full access to the SYSTEM group.
2. Distribute updates to other protected devices.
   - On each of the protected devices, configure the Application Database Update and Software Module Updates tasks.

a. For the update source, specify a folder on the intermediate device's drive to which updates will be downloaded.

b. Specify the folder where the updates will be saved.

> We recommend to deny access to the folder where updates are saved for all device user groups except for the Administrators and SYSTEM groups. We recommend to grant the Administrators group read, view, and run rights, and grant full access to the SYSTEM group.

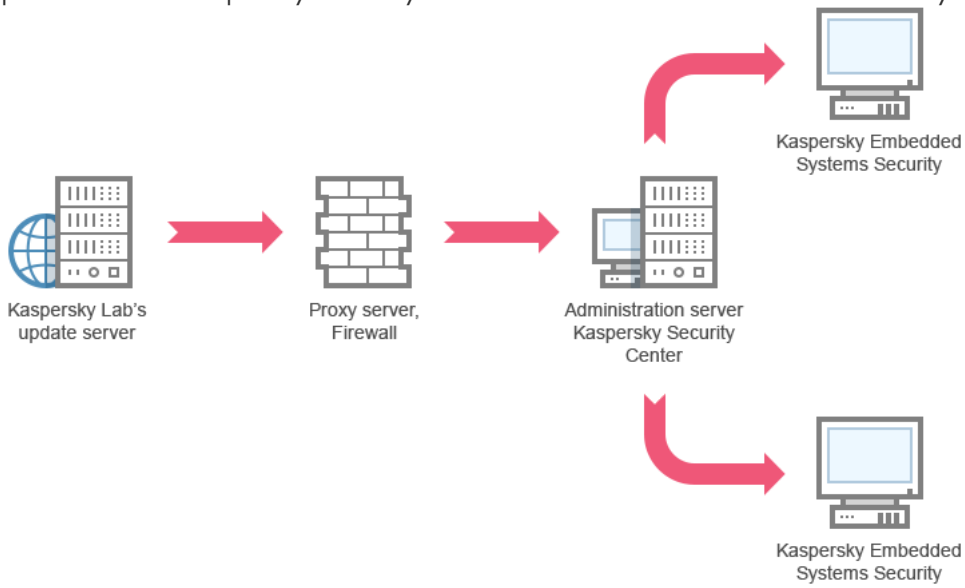
Kaspersky Embedded Systems Security for Windows will obtain updates via one of the protected devices.



Scheme 2: Updating databases and modules via one of the protected devices

Scheme 3. Updating databases and modules via Kaspersky Security Center Administration Server

If you are using Kaspersky Security Center to centrally manage antivirus protection for devices, you can download updates via the Kaspersky Security Center Administration Server installed on your local network.



Scheme 3: Updating databases and modules via Kaspersky Security Center Administration Server

To configure Kaspersky Embedded Systems Security for Windows updates via the Kaspersky Security Center Administration Server:

1. Install the Network Agent on each of the protected devices. The Network Agent is a software component included in the Kaspersky Security Center distribution kit. This ensures interaction between the Administration Server and Kaspersky Embedded Systems Security for Windows on the protected device. Detailed information about Network Agent and its configuration using Kaspersky Security Center is provided in the *Kaspersky Security Center Help*.

2. Download updates from Kaspersky update servers to Kaspersky Security Center Administration Server.

   - Configure the Retrieve Updates by Administration Server task for the specified set of protected devices:

     a. Specify Kaspersky's update server as the update source.

3. Distribute updates to protected devices. To do so, perform one of the following actions:

   - On the Kaspersky Security Center configure an Anti-Virus database (application module) update group task to distribute updates to protected devices:

     a. In the task schedule specify **After Administration Server has retrieved updates** as the start frequency.

     Administration Server will start the task each time it receives updates (recommended method).

     The **After Administration Server has retrieved updates** start frequency cannot be specified in the Application Console.

   - On each protected device, configure the Database Update task and the Software Modules Update task:

     a. Specify the Kaspersky Security Center Administration Server as the update source.

     b. Configure the task schedule if necessary.

     If Kaspersky Embedded Systems Security for Windows anti-virus databases are rarely updated (from once a month to once a year), the likelihood of detecting threats decreases and the frequency of false alarms raised by application components increases.

Kaspersky Embedded Systems Security for Windows will obtain updates via the Kaspersky Security Center Administration Server.

Scheme 4. Updating application databases from a secure removable drive

To update Kaspersky Embedded Systems Security for Windows databases from a secure removable drive:

1. Connect a Rutoken removable drive to the protected computer.

2. Add an allow rule to the Device Control task for the connected Rutoken removable drive.

3. In the Application Console on the device for which the most up-to-date antivirus databases are available, start, configure, and run the Secure Application Database Copy task. Select a Rutoken removable drive as the secure removable drive.

4. In the Application Console on the protected device where you need to update the application databases, start and run the Secure Application Database Update task. Select the connected Rutoken removable drive you copied the application databases to as the secure removable drive.

Kaspersky Embedded Systems Security for Windows will receive the updated application databases from the Rutoken secure removable drive.

Configuring Update tasks

This section contains instructions on how to configure update tasks for Kaspersky Embedded Systems Security for Windows via the Application Console.

You can also configure update tasks via the Administration Plug-in and Web Plug-in.

Configuring settings for working with Kaspersky Embedded Systems Security for Windows update sources

For each update task except the Rollback of Database Update task, you can specify one or more update sources, add user-defined update sources, and configure the settings for connecting to the specified sources.

After update task settings are modified, the new settings will not be immediately applied in running update tasks. The configured settings will be applied only when the task is restarted.

To specify the type of update source:

1. In the Application Console tree, expand the **Update** node.
2. Select the child node corresponding to the update task that you want to configure.
3. Click the **Properties** link in the results pane of the selected node.

   The **Task settings** window opens on the **General** tab.
4. In the **Update source** section, select the type of Kaspersky Embedded Systems Security for Windows update source:
   - Kaspersky Security Center Administration Server
   - Kaspersky update servers
   - Custom HTTP or FTP servers, or network folders
5. If required, configure the advanced settings for user-defined update sources:
   a. Click the **Custom HTTP or FTP servers, or network folders** link.
      1. In the **Update servers** window that opens, select or clear the check boxes next to user-defined update sources in order to start or stop using them.
      2. Click the **OK** button.

b. In the **Update source** section on the **General** tab, select or clear the **Use Kaspersky update servers if specified servers are not available** check box.

6. In the **Task settings** window, select the **Connection settings** tab to configure the settings for connecting to update sources:

   - Clear or select the **Use proxy server settings to connect to Kaspersky update servers** check box.
   - Clear or select the **Use proxy server settings to connect to other servers** check box.

   For information about configuring the optional proxy server settings and authentication settings for accessing the proxy server, see Starting and configuring Kaspersky Embedded Systems Security for Windows Database Update task section.

7. Click the **OK** button.

The configured settings for the Kaspersky Embedded Systems Security for Windows update source will be saved and applied at the next task start.

You can manage the list of user-defined Kaspersky Embedded Systems Security for Windows update sources.

To edit the list of user-defined application update sources:

1. In the Application Console tree, expand the **Update** node.
2. Select the child node corresponding to the update task that you want to configure.
3. Click the **Properties** link in the results pane of the selected node.

   The **Task settings** window opens on the **General** tab.

4. Click the **Custom HTTP or FTP servers, or network folders** link.

   The **Update servers** window opens.

5. Do the following:

   - To add a new user-defined update source, click **Add** and in the entry field specify the address of the folder containing update files on the FTP or HTTP server. Specify a local or network folder in the UNC (Universal Naming Convention) format. Press the **ENTER** key.

     By default, the added folder is used as the source of updates.

   - To disable use of a user-defined source, clear the check box next to the source in the list.
   - To enable use of a user-defined source, select the check box next to the source in the list.
   - In order to change the order in which Kaspersky Embedded Systems Security for Windows accesses user-defined update sources, use the **Move up** and **Move down** buttons to move the selected source toward the beginning or end of the list, depending on whether it is to be used before or after other sources.
   - To change the path to a user-defined source, select the source in the list and click the **Edit** button, make the required changes in the entry field, and press the **ENTER** key.
   - To remove a user-defined source, select it in the list and click the **Remove** button.

You cannot delete the only remaining user-defined source from the list.

6. Click the **OK** button.

The changes in the list of user-defined application update sources will be saved.

Optimizing disk I/O when running the Database Update task

When running the Database Update task, Kaspersky Embedded Systems Security for Windows stores update files on the protected device's local disk. You can lower the workload on the protected device's disk I/O subsystem by storing update files on a virtual drive in RAM when running the update task.

This feature is available for Microsoft Windows 7 operating systems and higher.

When using this feature while running the Database Update task, an extra logical drive may appear in the operating system. This logical drive will be removed from the operating system after the task is completed.

To lower the workload on your protected devices's disk I/O subsystem during the Database Update task:

1. In the Application Console tree, expand the **Update** node.
2. Select the **Database Update** child node.
3. Click the **Database Update** link in the results pane of the **Properties** node.

   The **Task settings** window opens on the **General** tab.
4. In the **Disk I/O usage optimization** section, define the following settings:

   - Clear or select the **Lower the load on the disk I/O** check box.
   - In the **RAM used for optimization, MB** field, specify the RAM volume (in MB). The operating system temporarily allocates the specified RAM volume to store update files while running the task. The default RAM size is 512 MB. The minimum RAM size is 400 MB.

     When running the Database Update task with the disk subsystem optimization feature enabled, one of the following may occur, depending on the amount of RAM allocated for the feature:

     - If the value is too small, the allocated amount of RAM might be insufficient to complete the database update task (for example, during the first update), which will lead to the completion of the task with an error.

       In this case, it is recommended to allocate more RAM for the disk subsystem optimization feature.
     - If the value is too large, at the start of the Database Update task, it might be impossible to create a virtual drive of a selected size in RAM. As a result, the disk subsystem optimization feature automatically disables, and the Database Update task runs without the optimization feature.

       In this case, it is recommended to allocate less RAM for the disk subsystem optimization feature.
5. Click the **OK** button.

The configured settings will be saved and applied at the next task start.

Configuring Copying Updates task settings

To configure the Copying Updates task:

1. In the Application Console tree, expand the **Update** node.
2. Select the **Copying Updates** child node.
3. Click the **Copying Updates** link in the results pane of the **Properties** node.
   The **Task settings** window appears.
4. On the **General** and **Connection settings** tabs, configure the settings for working with update sources.
5. On the **General** tab in the **Copying updates settings** section:
   - Specify the conditions for copying updates:
     - **Copy database updates**.
     - **Copy critical software modules updates**.
     - **Copy database updates and critical software modules updates**.
   - Specify the local or network folder to which Kaspersky Embedded Systems Security for Windows will be distributing downloaded updates.
6. On the **Schedule** and **Advanced** tabs, configure the task start schedule.
7. On the **Run as** tab, configure the task to start using a specific user account.
8. Click the **OK** button.

The configured settings will be saved and applied at the next task start.

Configuring Software Modules Update task settings

To configure the Software Modules Update task:

1. In the Application Console tree, expand the **Update** node.
2. Select the **Software Modules Update** child node.
3. Click the **Software Modules Update** link in the results pane of the **Properties** node.
   The **Task settings** window appears.
4. On the **General** and **Connection settings** tabs, configure the settings for working with update sources.
5. On the **General** tab in the **Update settings** section, configure the settings for updating application modules:
   - **Only check for available critical software modules updates**

- Copy and install critical software modules updates
- Allow operating system restart
- Receive information about available scheduled software modules updates

6. On the **Schedule** and **Advanced** tabs, configure the task start schedule. By default, Kaspersky Embedded Systems Security for Windows runs the Software Modules Update task on a weekly basis on Fridays at 4:00 PM (according to the regional time settings of the protected device).
7. On the **Run as** tab, configure the task to start using a specific user account.
8. Click the **OK** button.

The configured settings will be saved and applied at the next task start.

Kaspersky does not publish planned update packages on the update servers for automatic installation; these can be downloaded manually from the Kaspersky website. You can configure administrator notification about the *New critical and scheduled updates are available* event; the notification will contain the URL of the web page where scheduled updates can be downloaded.

Rolling back Kaspersky Embedded Systems Security for Windows database updates

Before database updates are performed, Kaspersky Embedded Systems Security for Windows creates backup copies of the previously used databases. If an update is interrupted or results in an error, Kaspersky Embedded Systems Security for Windows will automatically return to using the previously installed databases.

If any problems arise after you have updated the databases, you can roll back to the previously installed updates through the Rollback of Database Update task.

To start the Rollback of Database Update task:

In the results pane of the **Rollback of Application Database Update** node, click the **Start** link.

Rolling back application module updates

The names of settings may vary depending on the installed Windows operating system.

Before applying software module updates, Kaspersky Embedded Systems Security for Windows creates backup copies of the modules currently in use. If the module update process is interrupted or results in an error, Kaspersky Embedded Systems Security for Windows will automatically return to using modules from the latest installed updates.

In order to roll back software modules, use the **Install and delete applications** feature in Microsoft Windows.

Update task statistics

While the update task is running, the real-time information is displayed about the amount of data downloaded since the task started, as well as other task execution statistics.

When the task is complete or stopped, the information is available in the task log.

To view update task statistics:

1. In the Application Console tree, expand the **Update** node.
2. Select the child node that corresponds to the task whose statistics you want to view.

   Task statistics are displayed in the **Statistics** section of the results pane of the selected node.

If you are viewing/ the Database Update task or the Copying Updates task, the **Statistics** section shows the volume of data downloaded by Kaspersky Embedded Systems Security for Windows as of the present moment (**Received data**).

The following table contains the details for the Software Modules Update task.

Information about the Software Modules Update task

Field	Description
Received data	Total amount of downloaded data.
Available critical updates	Number of critical updates available for installation.
Available scheduled updates	Number of planned updates available for installation.
Errors applying updates	If the value of this field is non-zero, the update was not applied. The name of the update that resulted in an error can be viewed in the task log.

Isolating objects and copying backups

This section provides information about backing up detected malicious objects before they are disinfected or removed, and information about quarantining probably infected objects.

Isolating probably infected objects. Quarantine

This section describes how to isolate probably infected objects by quarantining them and how to configure Quarantine settings.

About quarantining probably infected objects

Kaspersky Embedded Systems Security for Windows quarantines probably infected objects by moving such objects from their original location to the *Quarantine* folder. For security purposes, objects in the Quarantine folder are stored in encrypted form.

Viewing quarantine objects

Quarantined objects can be viewed in the **Quarantine** node of the Application Console.

To view quarantined objects:

1. In the Application Console tree, expand the **Storages** node.
2. Select the **Quarantine** child node.

   Information about quarantined objects is displayed in the results pane of the selected node.

To find the required object in the list of quarantined objects,

sort the objects or filter the objects.

Sorting quarantined objects

By default, objects in the list of quarantined objects are sorted by quarantine date in reverse chronological order. To find the required object you may sort objects by the columns with object information. The sorted results will be saved if you close and then re-open the **Quarantine** node, or if you close the Application Console, save the msc file and then re-open it from this file.

To sort objects:

1. In the Application Console tree, expand the **Storages** node.
2. Select the **Quarantine** child node.

3. In the results pane of the **Quarantine** node, select the column heading that you wish to use to sort the objects in the list.

Objects in the list will be sorted based on the selected setting.

Filtering quarantined objects

To find the required quarantined object, you can filter objects in the list, i.e. display only those objects that satisfy the filtering criteria (filters) that you specify. The filtered results are saved if you close and then reopen the **Quarantine** node or if you close the Application Console, save the msc file and then reopen it from this file.

To specify one or more filters:

1. In the Application Console tree, expand the **Storages** node.
2. Select the **Quarantine** child node.
3. Select **Filter** in the context menu of the node's name.

   The **Filter settings** window opens.
4. To add a filter, perform the following steps:

   a. In the **Field name** list, select the field that will form the basis of the filter.

   b. In the **Operator** list, select the filtering condition. The filtering conditions in the list may differ depending on the value you selected in the **Field name** list.

   c. Enter the filter value in the **Field value** field or select a filter value.

   d. Click the **Add** button.

   The filter you added will appear in the list of filters in the **Filter settings** window. Repeat steps a-d for each filter you add. Follow these guidelines when working with filters:

   - To combine multiple filters using the logical operator "AND", select **If all conditions are met**.
   - To combine multiple filters using the logical operator "OR", select **If any condition is met**.
   - To delete a filter, select the filter you wish to delete in the filter list, and click the **Remove** button.
   - To edit a filter, select the filter in the list in the **Filter settings** window. Then change the required values in the **Field name**, **Operator** or **Field value** fields and click the **Replace** button.
5. After all filters have been added, click the **Apply** button.

The created filters will be saved.

To return to displaying all quarantined objects,

select **Quarantine** in the context menu of the **Remove filter** node.

Quarantine Scan

By default, after each database update, Kaspersky Embedded Systems Security for Windows performs the Quarantine Scan local system task. The task settings are described in the table below. The Quarantine Scan task settings cannot be modified.

You can configure the task start schedule, start the task manually, and modify the permissions of the account used to start the task.

After scanning quarantined objects following a database update, Kaspersky Embedded Systems Security for Windows may reclassify some of them as not infected: the status of such objects is changed to **False alarm**. Other objects may be reclassified as infected, in which case Kaspersky Embedded Systems Security for Windows handles such objects as specified by the Quarantine Scan task settings: disinfect, or delete if disinfection failed.

Quarantine Scan task settings

Quarantine Scan task setting	Value
Scan scope.	Quarantine folder
Security settings.	The same for the entire scan scope; their values are provided in the next table

Scan settings in the Quarantine Scan task

Security setting	Value
Scan objects	All objects included in the scan scope
Performance	Disabled
Action to perform on infected and other objects	Disinfect, delete if disinfection is impossible
Action to perform on probably infected objects	Skip
Exclude files	No
Do not detect	No
Stop scanning if it takes longer than (sec.)	Not defined
Do not scan objects larger than (MB)	Not defined
Scan alternate NTFS streams	Enabled
Scan disk boot sectors and MBR	Disabled
Use iChecker technology	Disabled
Use iSwift technology	Disabled
Scan compound objects	• **Archives*** • **SFX archives*** • **Packed objects*** • **Embedded OLE objects*** * **Scan only new and modified files** is disabled.
Check Microsoft signature in files	Not performed
Use heuristic analyzer	Enabled with **Deep** analysis level
Trusted Zone	Not applied

Restoring quarantined objects

Kaspersky Embedded Systems Security for Windows places probably infected objects into the Quarantine folder in encrypted form to shield the protected device against any possible harmful effects.

You can restore any object from Quarantine. This may be required in the following cases:

- After a Quarantine Scan using an updated database, the status of the object changes to **False alarm** or **Disinfected**.
- You consider the object harmless for the protected device and want to use it. If you do not want Kaspersky Embedded Systems Security for Windows to isolate the object during the subsequent scans, you can exclude the object from processing in the Real-Time File Protection task and On-Demand Scan tasks. To do this, specify the object in the **Exclude files** (by filename) or **Do not detect** security setting in those tasks, or add it to the Trusted Zone.

When you restore objects you can select where the object being restored will be saved: the original location (default), a special folder for restored objects on the protected device, or a custom folder on the protected device where the Application Console is installed, or on a different device on the network.

You can specify the folder for storing restored objects on the protected device. You can configure special security settings for it to be scanned. The path to this folder is set by the Quarantine settings.

Restoring objects from Quarantine may lead to an infection of the protected device.

You can restore the object and save a copy of it in the Quarantine folder to use later, for example, to rescan the object after the database has been updated.

If a quarantined object was contained in a compound object (for example, in an archive), Kaspersky Embedded Systems Security for Windows will not include the quarantined object when restoring the compound object. A quarantined object is saved separately in the selected folder.

You can restore one or more objects.

To restore quarantined objects, perform the following steps:

1. In the Application Console tree, expand the **Storages** node.
2. Select the **Quarantine** child node.
3. Perform one of the following actions in the details pane of the **Quarantine** node:
   - To restore one object, select **Restore** from the context menu of the object that you want to restore.
   - To restore multiple objects, select the objects you wish to restore using the **CTRL** or **SHIFT** key, right-click one of the selected objects, and select **Restore** from the context menu.

   The **Restore object** window opens.
4. In the **Restore object** window, specify the folder in which the object being restored will be saved for each selected object.

The name of the object is displayed in the **Object** field in the upper part of the window. If you selected several objects, the name of the first object in the list of selected objects will be displayed.

5. Do one of the following:

   - To restore an object to its original location, select **Restore to the source folder**.
   - To restore an object to the folder specified as the location for restored objects in the settings, select **Restore to the default folder for restoration**.
   - To save an object to a different folder on the protected device where the Application Console is installed, select **Restore to folder on your local computer** and then select the required folder or specify the path to it.

6. If you want to save a copy of the object in the *Quarantine* folder after the object is restored, clear the **Remove objects from storage after they are restored** check box.

7. To apply the specified restoration conditions to the rest of the selected objects, check the **Apply to all selected objects** box.

   All selected objects are restored and saved in the specified location. If you selected **Restore to the source folder**, each of the objects will be saved in its original location; if you selected **Restore to the default folder for restoration** or **Restore to folder on your local computer**, all objects will then be saved in one specified folder.

8. Click the **OK** button.

   Kaspersky Embedded Systems Security for Windows will start restoring the first of the selected objects.

9. If an object with this name already exists in the specified location, the **Object with this name already exists** window opens.

   a. Select one of the following Kaspersky Embedded Systems Security for Windows actions:

      - **Replace**, to replace the existing object with the restored object.
      - **Rename**, to save the restored object under a different name. In the entry field, enter the new restored object's filename and full path.
      - **Rename by adding suffix**, to rename the restored object by adding a suffix to its filename. Enter the suffix in the entry field.

   b. If you selected several objects to be restored, then select the **Rename** check box to apply the selected action (**Apply to all selected objects** or **Replace**) to the rest of the selected objects. If you selected **Rename**, the **Apply to all selected objects** check box will be unavailable.

   c. Click the **OK** button.

   The object will be restored. Information about the restoration operation will be recorded in the system audit log.

   If you did not select **Apply to all selected objects** in the **Restore object** window, the **Restore object** window may open again. Use this window to specify the location where the next selected object will be saved (see Step 4 of this procedure).

Moving objects to Quarantine

You can quarantine files manually.

To quarantine a file:

1. In the Application Console tree, open the context menu of the **Quarantine** node.
2. Select **Add**.
3. In the **Open** window, select the file on the disk that you wish to quarantine.
4. Click the **OK** button.

Kaspersky Embedded Systems Security for Windows will quarantine the selected file.

Deleting objects from Quarantine

Based on the Quarantine Scan task settings, Kaspersky Embedded Systems Security for Windows automatically deletes objects from the Quarantine folder if their status changed to *Infected* during a Quarantine Scan with updated databases and if Kaspersky Embedded Systems Security for Windows failed to disinfect them. Kaspersky Embedded Systems Security for Windows does not remove other objects from Quarantine.

One or more objects can be deleted from Quarantine.

To delete one or more objects from Quarantine:

1. In the Application Console tree, expand the **Storages** node.
2. Select the **Quarantine** child node.
3. Do one of the following:
   - To remove one object, select **Remove** in the context menu of the name of the object.
   - To delete multiple objects, select the objects that you want to delete using the **Ctrl** or **Shift** key, open the context menu on any one of the selected objects, and select **Remove**.
4. In the confirmation window, click the **Yes** button to confirm the operation.

The selected objects will be removed from Quarantine.

Sending probably infected objects to Kaspersky for analysis

If the behavior of a file gives you a reason to suspect that it contains a threat, and Kaspersky Embedded Systems Security for Windows considers the file to be clean, you may have encountered an unknown threat whose signature has not yet been added to the databases. You can send this file to Kaspersky for analysis. Kaspersky's Anti-Virus analysts will analyze it and, if they detect a new threat, will add a record identifying it in the databases. When you rescan the object after the database has been updated, it is likely that Kaspersky Embedded Systems Security for Windows will identify the object as infected and will be able to disinfect it. You will not only be able to keep the object, but will also prevent a virus outbreak.

Only quarantined files can be sent for analysis. Quarantined files are stored in encrypted form and are not deleted by the Anti-Virus application installed on the mail server when they are sent.

A quarantined object cannot be sent to Kaspersky for analysis after the license expires.

To send a file for analysis to Kaspersky:

1. If the file was not quarantined, first move it into **Quarantine**.
2. In the **Quarantine** node, open the context menu on the file you want to send for analysis and select **Send object for analysis** in the context menu.
3. In the confirmation window that opens, click **Yes** if you are sure you want to send the selected object for analysis.
4. If a mail client is configured on the protected device on which the Application Console is installed, a new email message is created. Review it and click the **Send** button.

   The **Receiver** field contains the Kaspersky email address newvirus@kaspersky.com. The Subject field will contain the text "Quarantined object".

   The body of the message will contain the following text: "This file will be sent to Kaspersky for analysis." Any additional information about the file, why you considered it probably infected or dangerous, how it behaves, or how it affects the system, can be included in the body of the message.

   An archive named <object name>.cab will be attached to the message. This archive will contain a <uuid>.klq file with the object in encrypted form, a <uuid>.txt file with object information received from Kaspersky Embedded Systems Security for Windows, and a Sysinfo.txt file that contains the following information about Kaspersky Embedded Systems Security for Windows and the operation system installed on the protected device:

   - Name and version of the operating system.
   - Name and version of Kaspersky Embedded Systems Security for Windows.
   - Release date of the latest database update installed.
   - Active key.

   This information is required by Kaspersky's anti-virus analysts to analyze your file faster and more efficiently. However, if you do not wish to send this information, you can delete the Sysinfo.txt file from the archive.

If a mail client is not installed on the protected device with the Application Console, the application prompts you to save the selected encrypted object to file. This file can be sent to Kaspersky manually.

To save an encrypted object to a file:

1. In the window that opens with a prompt to save the object, click **OK**.
2. Select a folder on the drive of the protected device or a network folder, where you want to save the file containing the object.

The object will be saved to a CAB file.

Configuring Quarantine settings

You can configure Quarantine settings. New Quarantine settings are applied immediately after saving.

To configure Quarantine settings:

1. In the Application Console tree, expand the **Storages** node.
2. Open the context menu of the **Quarantine** child node.
3. Select **Properties**.
4. In the **Quarantine: Properties** window, configure the necessary Quarantine settings in accordance with your requirements:
   - In the **Quarantine settings** section:
     - Quarantine folder
     - Maximum Quarantine size (MB)
     - Threshold value for space available (MB)

     If the size of objects in Quarantine exceeds the maximum quarantine size or exceeds the available space threshold, Kaspersky Embedded Systems Security for Windows will notify you about this while continuing to place objects in Quarantine.
   - In the **Restoration settings** section:
     - Target folder for restoring objects
5. Click the **OK** button.

The newly configured Quarantine settings will be saved.

Quarantine statistics

You can view information about the number of quarantined objects, i.e. quarantine statistics.

To view quarantine statistics,

in the context menu of the **Quarantine** node in the Application Console tree, select **Statistics**.

The **Quarantine statistics** window displays information about the number of objects currently stored in Quarantine (see the following table):

Field	Description
Probably infected objects	Number of objects found by Kaspersky Embedded Systems Security for Windows to be probably infected.
Used quarantine space	Total amount of data in the Quarantine folder.
False positives	The number of objects that received *False alarm* status because they were classified as non-infected during a Quarantine Scan using updated databases.
Objects	The number of objects that received *Disinfected* status after the Quarantine Scan.

disinfected	
Total number of objects	Total number of objects in Quarantine.

Making backup copies of objects. Backup

This section provides information about backup of detected malicious objects before disinfection or deletion, as well as instructions for configuring Backup.

About backing up objects before disinfection or deletion

Kaspersky Embedded Systems Security for Windows stores encrypted copies of objects classified as *Infected* in *Backup* before disinfecting or deleting them.

If the object is a part of a compound object (for example, part of an archive), Kaspersky Embedded Systems Security for Windows will save the compound object in its entirety in Backup. For example, if Kaspersky Embedded Systems Security for Windows has detected that one of the objects from a mail database is infected, it will back up the entire mail database.

Large objects placed in Backup by Kaspersky Embedded Systems Security for Windows can slow down the system and reduce available disk space on the hard drive.

Files can be restored from Backup either to their original folder or to a different folder on the protected device or on another device in the local area network. A file can be restored from Backup, for example, if an infected file contains important information, but Kaspersky Embedded Systems Security for Windows is unable to disinfect it without damaging its integrity and losing the information.

Restoring files from Backup may lead an infection of the protected device.

Viewing objects stored in Backup

Objects can be viewed in the Backup folder only by using the Application Console in the **Backup** node. They cannot be viewed using Microsoft Windows file managers.

To view the objects in Backup,

1. In the Application Console tree, expand the **Storages** node.
2. Select the **Backup** child node.

   Information about objects placed in Backup is displayed in the results pane of the selected node.

To find the necessary object in the list of objects in Backup,

sort the objects or filter the objects.

Sorting files in Backup

By default, files in Backup are sorted by the backup date in reverse chronological order. To find the required file, you can sort files according to the content of any column in the results pane.

The sorting result will be saved if you close and then re-open the **Backup** node or if you close the Application Console, save the msc file and then re-open it from this file.

To sort files in Backup:

1. In the Application Console tree, expand the **Storages** node.
2. Select the **Backup** child node.
3. In the list of files in the **Backup** node, select the column heading which you want to use to sort the objects.

   Files in Backup will be sorted based on the selected criterion.

Filtering files in Backup

To find the required file in Backup you can filter files: display in the **Backup** node only those files which satisfy the filtering criteria you have specified (filters).

The sorting result will be saved if you close and then re-open the **Backup** node or if you close the Application Console, save the msc file and then re-open it from this file.

To filter files in Backup:

1. In the Application Console tree, open the context menu of the **Backup** node and select **Filter**.

   The **Filter settings** window opens.
2. To add a filter, perform the following steps:

   a. In the **Field name** list, select the field that will form the basis of the filter.

   b. In the **Operator** list, select the filtering condition. The filtering conditions in the list may differ depending on the value you selected in the **Field name** field.

   c. Enter the filter value in the **Field value** field or select a filter value.

   d. Click the **Add** button.

   The filter you added will appear in the list of filters in the **Filter settings** window. Repeat these steps for each added filter. Follow these guidelines when working with filters:

   - To combine multiple filters using the logical operator "AND", select **If all conditions are met**.
   - To combine multiple filters using the logical operator "OR", select **If any condition is met**.
   - To delete a filter, select the filter you wish to delete in the filter list, and click the **Remove** button.

- To edit the filter, select it from the filter list in the **Filter settings** window, modify the required values in the **Field name**, **Operator**, and **Field value** fields, and click the **Replace** button.

When all filters have been added, click the **Apply** button. Only files that match the filters you have specified will be displayed in the list.

To display all files included in the list of objects stored in Backup,

select **Backup** in the context menu of the **Remove filter** node.

Restoring files from Backup

Kaspersky Embedded Systems Security for Windows stores files in the Backup folder in encrypted form to shield the protected device against possible harmful effects.

Any file can be restored from Backup.

A file may need to be restored in the following cases:

- The original infected file contained important information and Kaspersky Embedded Systems Security for Windows failed to keep its integrity so, as a result, the information in the file became unavailable.
- You consider the file harmless to the protected device and want to use it. If you do not want Kaspersky Embedded Systems Security for Windows to consider this file infected or probably infected, during subsequent scans you can exclude it from processing in the Real-Time File Protection task and On-Demand Scan tasks. To do this, specify the file in the **Exclude files** setting or the **Do not detect** setting in the corresponding tasks.

Restoring files from Backup may lead to an infection of the protected device.

When you restore a file you can select where it will be saved: the original location (default), a special folder for restored objects on the protected device, or a custom folder on the protected device where the Application Console is installed, or on a different device on the network.

You can specify the folder for storing restored objects on the protected device. You can configure special security settings for it to be scanned. The path to this folder is specified by the Backup settings.

By default when Kaspersky Embedded Systems Security for Windows restores a file, it makes a copy of it in Backup. The file copy can be deleted from Backup after it is restored.

To restore files from Backup:

1. In the Application Console tree, expand the **Storages** node.
2. Select the **Backup** child node.
3. Perform one of the following actions in the details pane of the **Backup** node:
   - To restore one object, select **Restore** from the context menu of the object that you want to restore.
   - To restore multiple objects, select the objects you wish to restore using the **CTRL** or **SHIFT** key, right-click one of the selected objects, and select **Restore** from the context menu.

   The **Restore object** window opens.

4. In the **Restore object** window, specify the folder in which the object being restored will be saved for each selected object.

   The name of the object is displayed in the **Object** field in the upper part of the window. If you selected several objects, the name of the first object in the list of selected objects will be displayed.

5. Do one of the following:

   - To restore an object to its original location, select **Restore to the source folder**.
   - To restore an object to the folder specified as the location for restored objects in the settings, select **Restore to the default folder for restoration**.
   - To save an object to a different folder on the protected device where the Application Console is installed, select **Restore to folder on your local computer** and then select the required folder or specify the path to it.

6. If you do not want to save a copy of the file in the Backup folder after it is restored, select the **Remove objects from storage after they are restored** check box (by default, this check box is cleared).

7. To apply the specified restoration conditions to the rest of the selected objects, check the **Apply to all selected objects** box.

   All selected objects are restored and saved in the specified location. If you selected **Restore to the source folder**, each of the objects will be saved in its original location; if you selected **Restore to the default folder for restoration** or **Restore to folder on your local computer**, all objects will then be saved in one specified folder.

8. Click the **OK** button.

   Kaspersky Embedded Systems Security for Windows will start restoring the first of the selected objects.

9. If an object with this name already exists in the specified location, the **Object with this name already exists** window opens.

   a. Select one of the following Kaspersky Embedded Systems Security for Windows actions:

      - **Replace**, to replace the existing object with the restored object.
      - **Rename**, to save the restored object under a different name. In the entry field, enter the new restored object's filename and full path.
      - **Rename by adding suffix**, to rename the restored object by adding a suffix to its filename. Enter the suffix in the entry field.

   b. If you selected several objects to be restored, then select the **Rename** check box to apply the selected action (**Apply to all selected objects** or **Replace**) to the rest of the selected objects. If you selected **Rename**, the **Apply to all selected objects** check box will be unavailable.

   c. Click the **OK** button.

   The object will be restored. Information about the restoration operation will be recorded in the system audit log.

If you did not select **Apply to all selected objects** in the **Restore object** window, the **Restore object** window may open again. Use this window to specify the location where the next selected object will be saved (see Step 4 of this procedure).

Deleting files from Backup

To delete one or more files from Backup:

1. In the Application Console tree, expand the **Storages** node.
2. Select the **Backup** child node.
3. Do one of the following:
   - To remove one object, select **Remove** in the context menu of the name of the object.
   - To delete multiple objects, select the objects that you want to delete using the **Ctrl** or **Shift** key, open the context menu on any one of the selected objects, and select **Remove**.
4. In the confirmation window, click the **Yes** button to confirm the operation.

The selected files will be deleted from Backup.

Configuring Backup settings

To configure Backup settings:

1. In the Application Console tree, expand the **Storages** node.
2. Open the context menu of the **Backup** child node.
3. Select **Properties**.
4. In the **Backup: Properties** window, configure the necessary Backup settings in accordance with your requirements:

   In the **Backup settings** section:

   - Backup folder
   - Maximum Backup size (MB)
   - Threshold value for space available (MB)

     If the size of objects in Backup exceeds the maximum Backup size or exceeds the available space threshold, Kaspersky Embedded Systems Security for Windows will notify you about this while continuing to place objects in Backup.

   In the **Restoration settings** section:

   - Target folder for restoring objects
5. Click the **OK** button.

The configured Backup settings will be saved.

Backup statistics

You can view information about the current status of Backup, i.e. Backup statistics.

To view Backup statistics,

open the context menu on the **Backup** node in the Application Console tree and select **Statistics**. The **Backup statistics** window opens.

The **Backup statistics** window displays information about the current Backup status (see the table below).

Information about the current Backup status

Field	Description
Current Backup size	Amount of data in the Backup folder; the application calculates the file size in encrypted form
Total number of objects	Current total number of objects in Backup

Blocking access to network resources. Blocked network sessions

This section describes how to block remote devices and configure the settings for the List of blocked network sessions.

List of blocked network sessions

By default, the List of blocked network sessions is available for use if any of the following components is installed: Real-Time File Protection, Network Threat Protection. These components discover remote attempts to encrypt, open or execute objects on the protected device or network attached storage shared folders in accordance with the list of blocked network sessions. Information about blocked network sessions from all protected devices is sent to the Kaspersky Security Center. Kaspersky Embedded Systems Security for Windows blocks current session and, in terms of current session, makes shared folders or network attached storage folders unavailable.

The List of blocked network sessions is populated when at least one of the following tasks is started in active mode (under specified conditions):

- For the Real-Time File Protection task: malicious activity by a device accessing network file resources is detected and in the Real-Time File Protection task settings the **Block access to network shared resources for the sessions that show malicious activity** check box is selected.
- For the Network Threat Protection task: activity typical of network attacks is detected.

After malicious activity or an encryption attempt is detected, the task sends information about the attacking network session to the List of blocked network sessions and the application creates a *Warning* event for current session of the attacking host. Any attempts by this session to access the protected shared network folders will be blocked.

If the locally unique identifier (LUID) of a host that initiated the attacking network session is added to the List of blocked network sessions, Kaspersky Embedded Systems Security for Windows determines the IP address of the host and adds it to the List of blocked network sessions instead of the LUID of the attacking host.

By default, Kaspersky Embedded Systems Security for Windows removes blocked network sessions from the list 30 minutes after they were added to the list. Access to network file resources is restored automatically after the network sessions are deleted from the List of blocked network sessions. You can specify the period of time after which blocked network sessions are automatically unblocked.

Note that when you restrict access to storage management for any user account, the List of blocked network sessions will still be available. The settings for blocked network sessions cannot be changed unless the selected user account has **Edit permissions** for managing Kaspersky Embedded Systems Security for Windows.

Managing the List of blocked network sessions via the Administration Plug-in

In this section, learn how to configure the settings for the List of blocked network sessions via the Administration Plug-in interface.

Enabling untrusted hosts blocking

To add network sessions showing any malicious or encryption activity to the **List of blocked network sessions** and block access to network file resources, at least one of the following tasks must be running in active mode:

- Real-Time File Protection
- Network Threat Protection

Configure the Real-Time File Protection task:

1. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node.
2. Select the **Policies** tab and open **<Policy name>** >**Real-Time Computer Protection** > **Settings** in the **Real-Time File Protection** block.

   The **Real-Time Computer Protection** window opens.
3. In the **Integration with other components** section, select the **List hosts showing malicious activity as untrusted** check box if you want Kaspersky Embedded Systems Security for Windows to block access to network file resources for hosts on which malicious activity is detected while the Real-Time File Protection task is running.
4. If the task has not been started, open the **Task management** tab:
   a. Select the **Run by schedule** check box.
   b. Select the **At application launch** frequency in the drop-down list.
5. In the **Real-Time Computer Protection** window, click **OK**.

The newly configured settings are saved.

Configure the Network Threat Protection task:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure the task.
3. Select the **Policies** tab.
4. Double-click the policy name you want to configure.
5. In the **Properties: <Policy name>** window that opens, select the section.
6. Click the **Settings** button in the **Network Threat Protection** subsection.
   The **Network Threat Protection** window opens.
7. Open the **General** tab.
8. In the **Operating mode** section select the **Block connections when attack is detected** processing mode.

   The check box enables or disables adding hosts showing activity typical of network attacks to the list of blocked hosts.

   If this mode is selected, Kaspersky Embedded Systems Security for Windows scans inbound network traffic for activity that is typical of network attacks, logs events about detected activity, and adds IP addresses of hosts showing activity typical of network attacks to the list of blocked hosts.

   You can view the list of blocked hosts in the Blocked Hosts storage.

   You can restore access to blocked hosts, and specify the number of days, hours, and minutes after which hosts regain access to network file resources after being blocked by configuring the Blocked Hosts storage settings.

   The mode is selected by default.

9. If the task has not been started, open the **Task management** tab:
   a. Select the **Run by schedule** check box.
   b. Select the **At application launch** frequency in the drop-down list.
10. In the window, click **OK**.
11. The newly configured settings are saved.

Configuring settings for the List of blocked network sessions

To configure the List of blocked network sessions:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.

3. Perform one of the following actions in the details pane of the selected administration group:

   - To configure application settings for a group of protected devices, select the **Policies** tab and open the **Properties: <Policy name>** window.

   - To configure the settings of a task or application for an individual protected device, select the **Devices** tab and go to local task settings or application settings.

4. In the **Supplementary** section, click the **Settings** button in the **Storages** subsection.

   The **Storages settings** window is displayed.

5. In the **Network session blocking terms** section of the **Blocked Network Sessions** tab, specify the number of days, hours and minutes after which blocked network sessions regain access to network file resources after being blocked.

6. Click the **OK** button.

Managing the List of blocked network sessions via the Application Console

In this section, learn how to configure the settings of the List of blocked network sessions via the Application Console interface.

Enabling untrusted hosts blocking

To add network sessions showing any malicious or encryption activity to the **List of blocked network sessions** and block access to network file resources, at least one of the following tasks must be running in active mode:

- Real-Time File Protection
- Network Threat Protection

Configure the Real-Time File Protection task:

1. In the Application Console tree, expand the **Real-Time Computer Protection** node.

2. Select the **Real-Time File Protection** child node.

3. Click the **Properties** link in the results pane.

   The **Task settings** window appears.

4. In the **Deep** section, select the **Block access to network shared resources for the sessions that show malicious activity** check box if you want Kaspersky Embedded Systems Security for Windows to block network sessions on which malicious activity is detected while the Real-Time File Protection task is running.

5. If the task has not been started, open the **Schedule** tab:

   a. Select the **Run by schedule** check box.

   b. Select the **At application launch** frequency in the drop-down list.

6. In the **Task settings** window, click **OK**.

The newly configured settings are saved.

Configure the Network Threat Protection task:

1. In the Application Console tree, expand the **Real-Time Computer Protection** node.
2. Select the **Network Threat Protection** child node.
3. Click the **Network Threat Protection** link in the details pane of the **Properties** node.
4. The **Task settings** window appears.
5. Open the **General** tab.
6. In the **Operating mode** section select the **Block connections when attack is detected** processing mode.

   The check box enables or disables adding hosts showing activity typical of network attacks to the list of blocked hosts.

   If this mode is selected, Kaspersky Embedded Systems Security for Windows scans inbound network traffic for activity that is typical of network attacks, logs events about detected activity, and adds IP addresses of hosts showing activity typical of network attacks to the list of blocked hosts.

   You can view the list of blocked hosts in the Blocked Hosts storage.

   You can restore access to blocked hosts, and specify the number of days, hours, and minutes after which hosts regain access to network file resources after being blocked by configuring the Blocked Hosts storage settings.

   The mode is selected by default.

7. Select or clear the **Don't stop traffic analysis when the task is not running** check box.

   If this check box is selected, then even when the Network Threat Protection task is stopped, Kaspersky Embedded Systems Security for Windows scans inbound network traffic for activity that is typical of network attacks and blocks network activity from the attacking computer, depending on the selected task mode.

   If this check box is cleared, when the Network Threat Protection task is stopped, Kaspersky Embedded Systems Security for Windows doesn't scan inbound network traffic for activity that is typical of network attacks.

   By default, the check box is cleared.

8. If the task has not been started, open the **Schedule** tab:
   a. Select the **Run by schedule** check box.
   b. Select the **At application launch** frequency in the drop-down list.
9. In the **Task settings** window, click **OK**.

The newly configured settings are saved.

Configuring settings for the List of blocked network sessions

To configure the List of blocked network sessions:

1. In the Application Console tree, expand the **Storages** node.
2. Open the context menu of the **Blocked network sessions** child node.
3. Select the **Properties** menu option.
   The **Settings for the List of blocked network sessions** window is displayed.
4. In the **Network session blocking term** section, specify the number of days, hours and minutes after which blocked network sessions regain access to network file resources after being blocked.
5. Click the **OK** button.
6. To restore access for all blocked network sessions:
   a. Open the context menu of the **Blocked network sessions** child node.
   b. Select the **Unblock all** option.
      All network sessions will be removed from the list and unblocked.
7. To remove several sessions from the list of blocked network sessions:
   a. In the list of blocked network sessions, which is displayed in the results pane, select one or more sessions.
   b. Open the context menu of the **Blocked network sessions** child node.
   c. Select the **Unblock selected** option.
      The selected network sessions are unblocked.

Managing the List of blocked network sessions via the Web Plug-in

In this section, learn how to configure the List of blocked network sessions settings via the Web Plug-in interface.

Enabling network sessions blocking

To add network sessions showing any malicious or encrypting activity to the **Blocked network sessions** and block access to network file resources for those sessions, at least one of the following tasks must run in the active mode:

- Real-Time File Protection
- Network Threat Protection

Configure the Real-Time File Protection task:

1. In the main window of the Web Console, select **Devices** → **Policies & profiles**.
2. Click the policy name you want to configure.

3. In the **<Policy name>** window that opens select the **Application settings** tab.

4. Select the **Real-time computer protection** section.

5. Click **Settings** in the **Real-Time File Protection** subsection.

6. In the **Integration with other components** section, select the **Block access to network shared resources for the sessions that show malicious activity** check box if you want Kaspersky Embedded Systems Security for Windows to block current session and make network shared resources unavailable for network sessions for which malicious activity was detected.

7. If the task has not been started, open the **Task management** tab:

   a. Select the **Run by schedule** check box.

   b. Select the **At application launch** frequency in the drop-down list.

8. Click the **Save** button.

The newly configured settings are saved.

Configuring settings for the List of blocked network sessions

To configure the List of blocked network sessions:

1. In the main window of the Web Console, select **Devices** → **Policies & profiles**.

2. Click the policy name you want to configure.

3. In the **<Policy name>** window that opens select the **Application settings** tab.

4. Select the **Supplementary** section.

5. Click the **Settings** button in the **Storages** subsection.

6. In the **Supplementary** section, click the **Settings** button in the **Storages** subsection.

   The **Storages** window is displayed.

7. In the **Network session blocking term** section of the **Blocked network sessions** tab, specify the number of days, hours and minutes after which blocked network sessions regain access to network file resources after being blocked.

8. Click the **OK** button.

Event registration. Kaspersky Embedded Systems Security for Windows logs

This section provides information about working with Kaspersky Embedded Systems Security for Windows logs.

Ways to register Kaspersky Embedded Systems Security for Windows events

Events of Kaspersky Embedded Systems Security for Windows are divided into two groups:

- Events related to the processing of objects in Kaspersky Embedded Systems Security for Windows tasks.
- Events related to the administration of Kaspersky Embedded Systems Security for Windows, such as starting the application, creating or deleting tasks, or editing task settings.

Kaspersky Embedded Systems Security for Windows uses the following methods to log events:

- **Task logs**. A task log contains information about the current task status and events that occurred during task execution.
- **System audit log**. The system audit log contains information about events related to the administration of Kaspersky Embedded Systems Security for Windows.
- **Event Log**. The Event Log contains information about events required to diagnose failures in the operation of Kaspersky Embedded Systems Security for Windows. The Event Log is available in Microsoft Windows Event Viewer.
- **Security log**. The Security log contains information about events associated with security breaches or attempted security breaches on the protected device.

If a problem occurs during operation of Kaspersky Embedded Systems Security for Windows (for example, Kaspersky Embedded Systems Security for Windows or an individual task terminates abnormally or does not start), you can create a trace file and a dump file of Kaspersky Embedded Systems Security for Windows processes and send files with this information to Kaspersky Technical Support for analysis in order to diagnose the problem.

Kaspersky Embedded Systems Security for Windows does not send any trace or dump files automatically. Diagnostic data can only be sent by a user who has the required permissions.

Kaspersky Embedded Systems Security for Windows writes information to trace files and the dump file in unencrypted form. The folder where files are saved is selected by the user and managed by the operating system configuration and Kaspersky Embedded Systems Security for Windows settings. You can configure access permissions and allow only required users to access logs, trace files and dump files.

Files that can be downloaded by the following links contain tables with the full lists of Kaspersky Embedded Systems Security for Windows events of the following categories:

- Events that Kaspersky Embedded Systems Security for Windows writes to the Event Log.

  DOWNLOAD KESS-WEL-EVENTS.ZIP

- Events that Kaspersky Embedded Systems Security for Windows sends to the Administration Server.

  DOWNLOAD KESS-KSC-EVENTS.ZIP

System audit log

Kaspersky Embedded Systems Security for Windows performs a system audit of events related to the administration of Kaspersky Embedded Systems Security for Windows. The application logs information about start of the application, starts and stops of Kaspersky Embedded Systems Security for Windows tasks, changes in task settings, and creation and deletion of On-Demand Scan tasks. Records of all those events are displayed in the results pane when you select the **System audit log** node in the Application Console.

By default, Kaspersky Embedded Systems Security for Windows stores records in the system audit log for an unlimited period of time. You can specify the storage period for records in the system audit log.

You can specify a folder that Kaspersky Embedded Systems Security for Windows will use to store files containing system audit log other than the default one.

Sorting events in the system audit log

By default, events in the system audit log node are displayed in reverse chronological order.

Events can be sorted by the contents of any column except the **Event** column.

To sort events in the system audit log:

1. In the Application Console tree, expand the **Logs and notifications** node.
2. Select the **System audit log** child node.
3. In the results pane, select the header of the column that you want to use to sort the events in the list.

   The sorted results will be saved for the next time you view the system audit log.

Filtering events in the system audit log

You can configure the system audit log to display only the records of events that meet the filtering conditions (filters) that you have specified.

To filter events in the system audit log:

1. In the Application Console tree, expand the **Logs and notifications** node.
2. Open the context menu of the **System audit log** child node and select **Filter**.

   The **Filter settings** window opens.
3. To add a filter, perform the following steps:

a. In the **Field name** list, select the column you want to use to filter events.

b. In the **Operator** list, select the filtering condition. Filtering conditions vary depending on the item selected in the **Field name** list.

c. In the **Field value**, select a value for the filter.

d. Click the **Add** button.

The filter you added will appear in the list of filters in the **Filter settings** window.

4. If necessary, perform one of the following actions:

   - To combine multiple filters using the logical operator "AND", select **If all conditions are met**.
   - To combine multiple filters using the logical operator "OR", select **If any condition is met**.

5. Click the **Apply** button to save the filtering conditions in the system audit log.

   The list of events of the system audit log displays only events that meet the filtering conditions. The filtered results will be saved for the next time you view the system audit log.

To disable the filter:

1. In the Application Console tree, expand the **Logs and notifications** node.
2. Open the context menu of the **System audit log** child node and select **Remove filter**.

   The list of events of the system audit log will then display all events.

Deleting events from the system audit log

By default, Kaspersky Embedded Systems Security for Windows stores records in the system audit log for an unlimited period of time. You can specify the storage period for records in the system audit log.

You can manually delete all events from the system audit log.

To delete events from the system audit log:

1. In the Application Console tree, expand the **Logs and notifications** node.
2. Open the context menu of the **System audit log** child node and select **Clear**.
3. Do one of the following:

   - If you want to save the contents of the log to a file in CSV or TXT format before deleting events from the system audit log, click the **Yes** button in the window asking you to confirm the deletion. In the window that opens, specify the name and location of the file.
   - If you do not want to save the contents of the log to a file, click the **No** button in the window asking you to confirm the deletion.

The system audit log will be cleared.

Task logs

This section provides information about Kaspersky Embedded Systems Security for Windows task logs and instructions on how to manage them.

About task logs

Information about the execution of Kaspersky Embedded Systems Security for Windows tasks is displayed in the results pane when you select the **Task logs** node in the Application Console.

In the log of each task, you can view task execution statistics, details of each of the objects that have been processed by the application since the task started, and task settings.

By default, Kaspersky Embedded Systems Security for Windows stores records in task logs for 30 days after a task is done. You can change the storage period for records in task logs.

You can specify a folder that Kaspersky Embedded Systems Security for Windows will use to store files containing task logs other than the default one. You can also select events that Kaspersky Embedded Systems Security for Windows will record in task logs.

Viewing the list of events in task logs

To view task logs:

1. In the Application Console tree, expand the **Logs and notifications** node.
2. Select the **Task logs** subnode.

   The list of events saved in Kaspersky Embedded Systems Security for Windows task logs will be displayed in the results pane.

Events can be sorted by any column or filtered.

Sorting task logs

By default, task logs are displayed in reverse chronological order. They can be sorted by any column.

To sort task logs:

1. In the Application Console tree, expand the **Logs and notifications** node.
2. Select the **Task logs** subnode.
3. In the results pane, select the header of the column that you want to use to sort Kaspersky Embedded Systems Security for Windows task logs.

The sorted results will be saved for the next time you view the task logs.

Filtering task logs

You can configure the list of task logs to display only the task logs that meet the filtering conditions (filters) that you have specified.

To filter task logs:

1. In the Application Console tree, expand the **Logs and notifications** node.
2. Open the context menu of the **Task logs** child node and select **Filter**.

   The **Filter settings** window opens.
3. To add a filter, perform the following steps:

   a. In the **Field name** list, select the column you want to use to filter task logs.

   b. In the **Operator** list, select the filtering condition. Filtering conditions vary depending on the item selected in the **Field name** list.

   c. In the **Field value**, select a value for the filter.

   d. Click the **Add** button.

   The filter you added will appear in the list of filters in the **Filter settings** window.
4. If necessary, perform one of the following actions:

   - To combine multiple filters using the logical operator "AND", select **If all conditions are met**.
   - To combine multiple filters using the logical operator "OR", select **If any condition is met**.
5. Click the **Apply** button to save the filtering conditions in the list of task logs.

The list of task logs displays only task logs that meet the filtering conditions. The filtered results will be saved for the next time you view the task logs.

To disable the filter:

1. In the Application Console tree, expand the **Logs and notifications** node.
2. Open the context menu of the **Task logs** child node and select **Remove filter**.

The list of task logs will then display all task logs.

Viewing statistics and information about a Kaspersky Embedded Systems Security for Windows task in task logs

In task logs, you can view detailed information about all events that have occurred in tasks since they started, as well as task execution statistics and task settings.

To view statistics and information about a Kaspersky Embedded Systems Security for Windows task:

1. In the Application Console tree, expand the **Logs and notifications** node.
2. Select the **Task logs** subnode.
3. In the details pane, open the **Logs** window using one of the following methods:
   - Double-click the task log you want to view.
   - Open the context menu of the task log you want to view and select **View log**.
4. In the window that opens, the following details are displayed:
   - The **Statistics** tab displays the time of task start and completion, as well as task statistics.
   - The **Events** tab displays a list of events logged during task execution.
   - The **Options** tab displays the task settings.
5. If necessary, click the **Filter** button to filter the events in the task log.
6. If necessary, click the **Export** button to export data from the task log into a file in CSV or TXT format.
7. Click the **Close** button.

The **Logs** window will be closed.

Exporting information from a task log

You can export data from a task log into a file in CSV or TXT format.

To export data from a task log:

1. In the Application Console tree, expand the **Logs and notifications** node.
2. Select the **Task logs** subnode.
3. In the details pane, open the **Logs** window using one of the following methods:
   - Double-click the task log you want to view.
   - Open the context menu of the task log you want to view and select **View log**.
4. In the lower part of the **Logs** window, click the **Export** button.
   The **Save as** window opens.
5. Specify the name, location, type, and encoding of the file to which you want to export data from the task log.
6. Click the **Save** button.

The specified settings are saved.

Deleting task logs

By default, Kaspersky Embedded Systems Security for Windows stores records in task logs for 30 days after a task is done. You can change the storage period for records in task logs.

You can manually delete task logs that are already complete.

Events from the logs of tasks that are currently running and tasks being used by other users will not be deleted.

To delete the task logs:

1. In the Application Console tree, expand the **Logs and notifications** node.
2. Select the **Task logs** subnode.
3. Do one of the following:
   - If you want to delete the logs of all tasks that are already complete, open the context menu of the **Task logs** child node and select **Clear**.
   - If you want to clear the log of an individual task, in the results pane, open the context menu the task log you want to clear, and select **Remove**.
   - If you want to clear the logs of several tasks:
     a. In the results pane, use the **Ctrl** or **Shift** key to select the task logs you want to clear.
     b. Open the context menu of any selected task log and select **Remove**.
4. Click the **Yes** button in the deletion confirmation window to confirm that you want to delete the logs.

The task logs that you selected will be cleared. The deletion of task logs will be recorded in the system audit log.

Security log

Kaspersky Embedded Systems Security for Windows maintains a log of events associated with security breaches or attempted security breaches on the protected device. The following events are recorded in this log:

- Exploit Prevention events.
- Critical Log Inspection events.
- Critical events that indicate an attempted security breach (for the Real-Time Computer Protection, On-Demand Scan, File Integrity Monitor, Applications Launch Control, and Device Control tasks).

You can clear the Security log. Moreover, Kaspersky Embedded Systems Security for Windows records a system audit event when the Security log is cleared.

Viewing the event log of Kaspersky Embedded Systems Security for Windows in Event Viewer

You can view the event log of Kaspersky Embedded Systems Security for Windows using the Microsoft Windows Event Viewer snap-in for Microsoft Management Console. The log contains events registered by Kaspersky Embedded Systems Security for Windows and required to diagnose failures in its operation.

Events that will be registered in the event log can be selected based on the following criteria:

- **by event types**.
- **by level of detail**. The level of detail corresponds to the importance level of the events registered in the log (informational, important, or critical events). The most detailed is the Informational level, which registers all events. The least detailed is the Critical level, which registers only critical events.

To view the Kaspersky Embedded Systems Security for Windows event log:

1. Click the **Start** button, enter the `mmc` command at the search bar, and press **ENTER**.

   Microsoft Management Console opens.

2. Select **File** > **Add or remove snap-in**.

   The **Add or remove snap-ins** window opens.

3. In the list of available snap-ins, select the **Event Viewer snap-in** and click the **Add** button.

   The **Select computer** window opens.

4. In the **Select computer** window, specify the protected device on which Kaspersky Embedded Systems Security for Windows is installed, and click **OK**.

5. In the **Add and remove snap-ins** window, click **OK**.

   In the Microsoft Management Console tree, the **Event Viewer** node appears.

6. Expand the **Event Viewer** node and select the **Applications and Services Logs** > **Kaspersky Embedded Systems Security for Windows** child node.

The Kaspersky Embedded Systems Security for Windows event log opens.

Configuring log settings via the Application Console

You can edit the following settings of Kaspersky Embedded Systems Security for Windows logs:

- Length of the storage period for events in task logs and the system audit log.
- Location of the folder in which Kaspersky Embedded Systems Security for Windows stores task log files and the system audit log file.
- Events generation thresholds for *Application database is out of date*, *Application database is extremely out of date* and *Critical areas scan has not been performed for a long time*.
- Events that Kaspersky Embedded Systems Security for Windows saves in task logs, the system audit log, and the event log of Kaspersky Embedded Systems Security for Windows in Event Viewer.
- Settings for publishing audit events and task performance events to the syslog server via the Syslog protocol.

To configure log settings using the Application Console:

1. In the Application Console tree, open the context menu of the **Logs and notifications** node and select **Properties**.

   The **Logs and notifications settings** window opens.

2. On the **General** tab, if necessary, select events that Kaspersky Embedded Systems Security for Windows will save in task logs, the system audit log, and the event log of Kaspersky Embedded Systems Security for Windows in Event Viewer:

   a. In the **Component** list, select the component of Kaspersky Embedded Systems Security for Windows for which you want to set the detail level.

   b. In the **Importance level** list, select a detail level for events in task logs, the system audit log, and the event log for the selected component.

      In the following table with a list of events, the check boxes are selected next to events that are registered in task logs, the system audit log, and the event log, according to the current detail level.

   c. If you want to manually enable registration of specific events for a selected component or task:

      1. In the **Importance level** list, select **Custom**.

      2. In the table with the list of events, select the check boxes next to events that you want to be registered in task logs, the system audit log, and the event log.

3. On the **Advanced** tab, configure the log storage settings and event generation thresholds for device protection status:

   - In the **Log storage** block:

     - **Logs folder**

     - **Remove task logs older than (days)**

     - **Remove from the system audit log events older than (days)**

   - In the **Event generation thresholds** block, specify the number of days after which the *Application database is out of date*, *Application database is extremely out of date*, and *Critical areas scan has not been performed for a long time* events will occur.

4. On the **SIEM integration** tab, configure the settings for publishing audit events and task performance events to the syslog server.

5. Click the **OK** button to save the changes.

About SIEM integration

To reduce the load on low-performance devices and to reduce the risk of system degradation as a result of increased application log sizes, you can configure the publication of audit events and task performance events to the *syslog server* via the Syslog protocol.

A syslog server is an external server for aggregating events (SIEM). It stores and analyzes received events and performs other log management actions.

You can use SIEM integration in two modes:

- Duplicate events on the syslog server: in this mode, all task performance events whose publication is configured in log settings, as well as all system audit events, continue to be stored on the protected device even after they are sent to the SIEM server.

  We recommend that you use this mode to reduce the load on the protected device as much as possible.

- Delete local copies of events: in this mode, all events that are registered during application operation and published to the SIEM server will be deleted from the protected device.

  > The application never deletes local versions of the security log.

Kaspersky Embedded Systems Security for Windows can convert events in application logs into formats supported by the syslog server so that those events can be transmitted and successfully recognized by the SIEM server. The application supports conversion into structured data format and into JSON format.

We recommend that you select the format of events based on the configuration of the utilized SIEM server.

Reliability settings

You can reduce the risk that events will be relayed to the SIEM server unsuccessfully by defining the settings for connecting to a mirror syslog server.

A mirror syslog server is an additional syslog server to which the application switches automatically if the connection to the main syslog server is unavailable or if the main server cannot be used.

Kaspersky Embedded Systems Security for Windows also uses system audit events to notify you about unsuccessful attempts to connect to the SIEM server and about errors while sending events to the SIEM server.

Configuring SIEM integration settings

By default, SIEM integration is not used. You can enable and disable SIEM integration, and configure relevant settings (see the table below).

SIEM integration settings

Setting	Default value	Description
Send events to a remote syslog server via syslog protocol	Not applied	You can enable or disable SIEM integration by selecting or clearing the check box, respectively.
Remove local copies for events that have been sent to a remote syslog server	Not applied	You can configure the settings for storing local copies of logs after they are sent to the SIEM server by selecting or clearing the check box.
Events format	Structured data	You can select one of two formats to which the application converts its events prior to sending them to the syslog server for better recognition of these events by the SIEM server.
Connection protocol	TCP	You can use the drop-down list to configure the connection to the main and mirror syslog servers via the UDP or TCP protocols.
Main syslog server connection settings	IP address: 127.0.0.1	You can use the appropriate fields to configure the IP address and port used to connect to the main syslog server.

	Port: 514	You can specify the IP address only in IPv4 format.
Use mirror syslog server if the main server is not accessible	Not applied	You can use the check box to enable or disable the use of a mirror syslog server.
Mirror syslog server connection settings	IP address: 127.0.0.1 Port: 514	You can use the appropriate fields to configure the IP address and port used to connect to the mirror syslog server. You can specify the IP address only in IPv4 format.

To configure the settings for integration with SIEM:

1. In the Application Console tree, open the context menu of the **Logs and notifications** node.
2. Select **Properties**.

   The **Logs and notifications settings** window opens.
3. Select the **SIEM integration** tab.
4. In the **Integration settings** block, select the **Send events to a remote syslog server via syslog protocol** check box.
5. If necessary, in the **Integration settings** block, select the **Remove local copies for events that have been sent to a remote syslog server** check box.

   The status of the **Remove local copies for events that have been sent to a remote syslog server** check box does not affect the settings for storing events of the security log: the application never automatically deletes security log events.
6. In the **Events format** block, specify the format to which you want to convert application events so that they can be sent to the SIEM server.

   By default, the application converts them into a structured data format.
7. In the **Connection settings** block:
   - Specify the SIEM connection protocol.
   - In the fields of the same name, specify the IPv4 address and port for connecting to the main syslog server.
   - Select the **Use mirror syslog server if the main server is not accessible** check box if you want the application to use other connection settings when unable to send events to the main syslog server.
   - In the fields of the same name, specify the IPv4 address and port for connecting to an additional syslog server.
8. Click the **OK** button.

   The configured SIEM integration settings will be applied.

Configuring logs and notifications settings via the Administration Plug-in

The Kaspersky Security Center Administration Console can be used to configure notifications for administrator and users about the following events in the operation of Kaspersky Embedded Systems Security for Windows and the anti-virus protection status on the device:

- The administrator can receive information about events of selected types.
- LAN users who access the protected device and terminal protected device users can receive information about *Object detected* events.

Notifications about Kaspersky Embedded Systems Security for Windows events can be configured either for a single protected device using the **Properties: <Protected device name>** window of the selected protected device, or for a group of protected devices in the **Properties: <Policy name>** window of the selected administration group.

On the **Event notifications** tab or in the **Notification settings** window, you can configure the following types of notifications:

- Administrator notifications about events of selected types can be configured using the **Event notifications** tab (the standard tab in Kaspersky Security Center). For details on notification methods, see the *Kaspersky Security Center Help*.
- Both administrator and user notifications can be configured in the **Notification settings** window.

You can configure notifications for some event types only in the window or on the tab; you can use both the window and tab to configure notifications for other event types.

If you configure notifications about events of the same type using the same mode on the **Event notifications** tab and in the **Notification settings** window, the system administrator will receive notifications for those events twice but in the same mode.

Configuring task logs settings

To configure Kaspersky Embedded Systems Security for Windows logs, perform the following steps:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
   - To configure log settings for a group of protected devices, select the **Policies** tab and open the **Properties: <Policy name>** window.
   - To configure the application for an individual protected device, select the **Devices** tab and go to the application settings.
4. In the **Logs and notifications** section, click the **Settings** button in the **Task logs** subsection.
5. The **Logs settings** window opens on the **Logs** tab.
6. Configure the level of detail of events in logs:
   a. In the **Component** list, select the component of Kaspersky Embedded Systems Security for Windows for which you want to set the detail level.

b. In the **Importance level** list, select a detail level for events in task logs, the system audit log, and the event log for the selected component.

In the following table with a list of events, the check boxes are selected next to events that are registered in task logs, the system audit log, and the event log, according to the current detail level.

c. If you want to manually enable registration of specific events for a selected component or task:

1. In the **Importance level** list, select **Custom**.

2. In the table with the list of events, select the check boxes next to events that you want to be registered in task logs, the system audit log, and the event log.

7. In the **Log storage** block, configure the log storage settings:

- **Logs folder**
- **Remove task logs older than (days)**
- **Remove from the system audit log events older than (days)**

8. On the **SIEM integration** tab, configure the settings for publishing audit events and task performance events to the syslog server.

9. Click the **OK** button.

The configured log settings are saved.

Security log

Kaspersky Embedded Systems Security for Windows maintains a log of events associated with security breaches or attempted security breaches on the protected device. The following events are recorded in this log:

- Exploit Prevention events.
- Critical Log Inspection events.
- Critical events that indicate an attempted security breach (for the Real-Time Computer Protection, On-Demand Scan, File Integrity Monitor, Applications Launch Control, and Device Control tasks).

You can clear the Security log. Moreover, Kaspersky Embedded Systems Security for Windows records a system audit event when the Security log is cleared.

Configuring SIEM integration settings

To reduce the load on low-performance devices and to reduce the risk of system degradation as a result of increased application log sizes, you can configure the publication of audit events and task performance events to the *syslog server* via the Syslog protocol.

A syslog server is an external server for aggregating events (SIEM). It stores and analyzes received events and performs other log management actions.

You can use SIEM integration in two modes:

- Duplicate events on the syslog server: in this mode, all task performance events whose publication is configured in log settings, as well as all system audit events, continue to be stored on the protected device even after they are sent to the SIEM server.

  We recommend that you use this mode to reduce the load on the protected device as much as possible.

- Delete local copies of events: in this mode, all events that are registered during application operation and published to the SIEM server will be deleted from the protected device.

  > The application never deletes local versions of the security log.

Kaspersky Embedded Systems Security for Windows can convert events in application logs into formats supported by the syslog server so that those events can be transmitted and successfully recognized by the SIEM server. The application supports conversion into structured data format and into JSON format.

You can reduce the risk that events will be relayed to the SIEM server unsuccessfully by defining the settings for connecting to a mirror syslog server.

A mirror syslog server is an additional syslog server to which the application switches automatically if the connection to the main syslog server is unavailable or if the main server cannot be used.

By default, SIEM integration is not used. You can enable and disable SIEM integration, and configure relevant settings (see the table below).

SIEM integration settings

Setting	Default value	Description
Send events to a remote syslog server via syslog protocol	Not applied	You can enable or disable SIEM integration by selecting or clearing the check box, respectively.
Remove local copies for events that have been sent to a remote syslog server	Not applied	You can configure the settings for storing local copies of logs after they are sent to the SIEM server by selecting or clearing the check box.
Events format	Structured data	You can select one of two formats to which the application converts its events prior to sending them to the syslog server for better recognition of these events by the SIEM server.
Connection protocol	TCP	You can use the drop-down list to configure the connection to the main syslog server via the UDP or TCP protocols, and to the mirror syslog server via the TCP protocol.
Main syslog server connection settings	IP address: 127.0.0.1 Port: 514	You can use the appropriate fields to configure the IP address and port used to connect to the main syslog server. You can specify the IP address only in IPv4 format.
Use mirror syslog server if the main server is not accessible	Not applied	You can use the check box to enable or disable the use of a mirror syslog server.
Mirror syslog server connection settings	IP address: 127.0.0.1 Port: 514	You can use the appropriate fields to configure the IP address and port used to connect to the mirror syslog server. You can specify the IP address only in IPv4 format.

To configure the settings for integration with SIEM:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.

2. Select the administration group for which you want to configure application settings.

3. Perform one of the following actions in the details pane of the selected administration group:

   - To configure log settings for a group of protected devices, select the **Policies** tab and open the **Properties: <Policy name>** window.

   - To configure the application for an individual protected device, select the **Devices** tab and go to the application settings.

4. In the **Logs and notifications** section, click the **Task logs** button in the **Settings** subsection.

   The **Logs and notifications settings** window opens.

5. Select the **SIEM integration** tab.

6. In the **Integration settings** block, select the **Send events to a remote syslog server via syslog protocol** check box.

7. If necessary, in the **Integration settings** block, select the **Remove local copies for events that have been sent to a remote syslog server** check box.

   The status of the **Remove local copies for events that have been sent to a remote syslog server** check box does not affect the settings for storing events of the security log: the application never automatically deletes security log events.

8. In the **Events format** block, specify the format to which you want to convert application events so that they can be sent to the SIEM server.

   By default, the application converts them into a structured data format.

9. In the **Connection settings** block:

   - Specify the SIEM connection protocol.

   - In the fields of the same name, specify the IPv4 address and port for connecting to the main syslog server.

   - Select the **Use mirror syslog server if the main server is not accessible** check box if you want the application to use other connection settings when unable to send events to the main syslog server.

   - In the fields of the same name, specify the IPv4 address and port for connecting to an additional syslog server.

10. Click the **OK** button.

The configured SIEM integration settings will be applied.

Configuring notification settings

To configure Kaspersky Embedded Systems Security for Windows notifications:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.

2. Select the administration group for which you want to configure application settings.

3. Perform one of the following actions in the details pane of the selected administration group:

   - To configure application settings for a group of protected devices, select the **Policies** tab and open the **Properties: <Policy name>** window.

   - To configure the settings of a task or application for an individual protected device, select the **Devices** tab and go to local task settings or application settings.

4. In the **Logs and notifications** section, click the **Event notifications** button in the **Settings** subsection.

5. In the **Notification settings** window, define the following settings of Kaspersky Embedded Systems Security for Windows according to your requirements:

   - In the **Notification settings** list select the type of notification whose settings you want to configure.

   - In the **Notify users** section configure the user notification method. If necessary, enter the text of the notification message.

   - In the **Notify administrators** section configure the administrator notification method. If necessary, enter the text of the notification message. If necessary, configure additional notification settings by clicking the **Settings** button.

   - In the **Event generation thresholds** section, specify the time intervals after which Kaspersky Embedded Systems Security for Windows logs *Application database is out of date*, *Application database is extremely out of date* and *Critical areas scan has not been performed for a long time* events.

     - **Application database is out of date (days)**

     - **Application database is extremely out of date (days)**

     - **Critical areas scan has not been performed for a long time (days)**

6. Click the **OK** button.

The configured notification settings are saved.

Configuring interaction with the Administration Server

To select the types of objects about which Kaspersky Embedded Systems Security for Windows sends information to the Kaspersky Security Center Administration Server:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.

2. Select the administration group for which you want to configure application settings.

3. Perform one of the following actions in the details pane of the selected administration group:

   - To configure application settings for a group of protected devices, select the **Policies** tab and open the **Properties: <Policy name>** window.

   - To configure the settings of a task or application for an individual protected device, select the **Devices** tab and go to local task settings or application settings.

4. In the **Logs and notifications** section, click the **Interaction with Administration Server** button in the **Settings** subsection.

   The **Administration Server Network lists** window opens.

5. In the **Administration Server Network lists** window, choose the types of objects about which Kaspersky Embedded Systems Security for Windows will send information to the Kaspersky Security Center Administration Server:

   - Quarantined objects.
   - Backed up objects.

6. Click the **OK** button.

   Kaspersky Embedded Systems Security for Windows will send information about the selected object types to the Administration Server.

Notification settings

This section provides information about ways in which users and administrators of Kaspersky Embedded Systems Security for Windows can be notified about application events and the device protection status, as well as instructions on how to configure notifications.

Administrator and user notification methods

You can configure the application to notify the administrator and users who access the device about the following events in the operation of Kaspersky Embedded Systems Security for Windows and the anti-virus protection status on the device.

- The administrator can receive information about events of selected types.
- LAN users who access a device and terminal device users can receive information about events of the *Object detected* type in the Real-Time File Protection task.

In the Application Console, administrator or user notifications can be activated using several methods:

- User notification methods:
  a. Terminal service tools.
     You can apply this method for notifying terminal protected device users if the protected device is used as terminal.
  b. Message service tools.
     You can apply this method for notification via Microsoft Windows message services.
- Administrator notification methods:
  a. Message service tools.
     You can apply this method for notification via Microsoft Windows message services.
  b. Running an executable file.
     This method runs an executable file stored on the protected device's local drive when an event occurs.
  c. Sending by email.
     This method uses email to transmit messages.

You can create the text of a message for individual event types. It can include an information field to describe an event. By default, the application uses a default message to notify users.

Configuring administrator and user notifications

Event notification settings give you a choice of methods for configuring and composing a message text.

To configure event notification settings:

1. In the Application Console tree, open the context menu of the **Logs and notifications** node and select **Properties**.

The **Logs and notifications settings** window opens.

2. On the **Notifications** tab select the notification mode:

   a. Select the event for which you wish to select a notification method from the **Event type** list.

   b. In the **Notify administrators** or **Notify users** group settings, select the check box next to the notification methods that you wish to configure.

   > You can only configure user notifications for the following events: **Object detected**, **Untrusted external device detected and restricted** event, and **Network session listed as untrusted** event.

3. To add the text of a message:

   a. Click the **Message text** button.

   b. In the window that opens, enter the text to be displayed in the corresponding event message.

   > You can create the same message for several event types: after selecting a notification method for one event type, use the **Ctrl** or **Shift** key to select the other event types for which you want to use the same message, and then click the **Message text** button.

   a. To add fields with information about an event, click the **Macro** button and select the relevant fields from the drop-down list. Fields with event information are described in the table in this section.

   b. To restore the default event message text, click the **By default** button.

4. To configure how administrators will be notified about a selected event, select the **Notifications** tab, and in the **Settings** section, click the **Notify administrators** button. Then, in the **Advanced settings** window, configure the selected notification methods. To do this, perform the following actions:

   a. For email notifications, open the **Email** tab and specify the email addresses of recipients (delimit addresses with semicolon), name or network address of the SMTP server, and port number in the appropriate fields. If necessary, specify the text that will be displayed in the **Subject** and **From** fields. The text in the **Subject** field can also include variables with information about the event (see table below).

   If you want to apply user account authentication when connecting to the SMTP server, select **Authentication settings** in the **Use SMTP authentication** group and specify the name and password of the user whose user account will be authenticated.

   b. For notifications using Windows Messenger Service, create a list of recipient protected devices for notifications on the **Windows Messenger Service** tab: for each protected device that you wish to add, click the **Add** button and enter its network name in the input field.

   c. To run an executable file, on the **Executable file** tab, select a file on the local drive of the protected device or enter the full path to it. This file will be run on the protected device when the event occurs. Enter the user name and password which will be used to execute the file.

   System environment variables can be used when the path to the executable file is specified; user environment variables are not allowed.

   If you wish to limit the number of messages of one event type over a period of time, on the **Advanced** tab, select **Do not send the same notification more than** and specify the number of times and a time interval.

5. Click the **OK** button.

The configured notification settings are saved.

Fields with event information

Variable	Description
%EVENT_TYPE%	Event type.
%EVENT_TIME%	Event time.
%EVENT_SEVERITY%	Importance level.
%OBJECT%	Object name (in Real-Time Computer Protection and On-Demand Scan tasks). The Software Modules Update task includes the name of the update and the address of the web page with information on the update.
%VIRUS_NAME%	The name of the object according to the Virus Encyclopedia classification. This name is included in the full name of a detected object that Kaspersky Embedded Systems Security for Windows returns on detecting an object. You can view the full name of a detected object in the task log.
%VIRUS_TYPE%	The type of detected object according to the Kaspersky classification, such as "virus" or "trojan". It is included in the full name of a detected object, which is returned by Kaspersky Embedded Systems Security for Windows when it finds an object infected or probably infected. You can view the full name of a detected object in the task log.
%USER_COMPUTER%	In Real-time File Protection tasks, the name of the protected device of the user who accessed the object on the device.
%USER_NAME%	In Real-Time File Protection tasks, the name of the user who accessed the object on the device.
%FROM_COMPUTER%	Name of the protected device where the notification originated.
%EVENT_REASON%	Reason the event occurred (some events do not have this field).
%ERROR_CODE%	Error code (only for the "internal task error" event).
%TASK_NAME%	Task name (only for events related to task performance).

Starting and stopping Kaspersky Embedded Systems Security for Windows

This section contains information about starting Application Console and about starting and stopping the Kaspersky Security Service.

Starting the Kaspersky Embedded Systems Security for Windows Administration Plug-in

No additional actions are required to start the Kaspersky Embedded Systems Security for Windows Administration Plug-in in Kaspersky Security Center. Once the Administration Plug-in is installed on the administrator's protected device, it is started together with Kaspersky Security Center. Detailed information about starting Kaspersky Security Center can be found in the *Kaspersky Security Center Help*.

Starting the Kaspersky Embedded Systems Security for Windows Console from the Start menu

The names of settings may vary depending on the installed Windows operating system.

*To start the Application Console from the **Start** menu:*

1. In the **Start** menu, select **Programs** > **Kaspersky Embedded Systems Security for Windows** > **Administration Tools** > **Kaspersky Embedded Systems Security for Windows Console**.

To add other snap-ins to the Application Console, start the Application Console in author mode.

To start the Application Console in author mode:

1. In the **Start** menu, select **Programs** > **Kaspersky Embedded Systems Security for Windows** > **Administration Tools**.
2. In the context menu of the Application Console, select the **Author** command.

   The Application Console is started in author mode.

If the Application Console has been started on the protected device, the Application Console window opens.

If you started the Application Console on a non-protected device, connect to the protected device.

To connect to the protected device:

1. In the Application Console tree, open the context menu of the **Kaspersky Embedded Systems Security for Windows** node.
2. Select the **Connect to another computer** command.

   The **Select protected device** window opens.
3. Select **Another device** in the window that opens.

4. Specify the network name of the protected device in the entry field on the right.

5. Click the **OK** button.

The Application Console will connect to the protected device.

If the user account that you are using to log in to Microsoft Windows does not have sufficient permissions to access the Kaspersky Security Management Service on the protected device, select the **Connect as user** check box and specify a different user account that the required permissions.

Starting and stopping the Kaspersky Security Service

By default, the Kaspersky Security Service starts automatically immediately after the operating system. The Kaspersky Security Service manages the work processes that execute the Real-Time Computer Protection, Computer Control, On-Demand Scan and update tasks.

By default when Kaspersky Embedded Systems Security for Windows is started, the Real-Time File Protection and Scan at Operating System Startup tasks are started, as well as other tasks that are scheduled to start **At application launch**.

If the Kaspersky Security Service is stopped, all running tasks are stopped. After you restart the Kaspersky Security Service, the application automatically starts only those tasks scheduled to run **At application launch**. Other tasks must be started manually.

You can start and stop the Kaspersky Security Service using the context menu of the **Kaspersky Embedded Systems Security for Windows** node or using the Microsoft Windows Services snap-in.

You can start and stop Kaspersky Embedded Systems Security for Windows if you are a member of the Administrators group on the protected device.

To stop or start the application using the Application Console:

1. In the Application Console tree, open the context menu of the **Kaspersky Embedded Systems Security for Windows** node.

2. Select one of the following items:

   - **Stop the service**

   - **Start the service**

The Kaspersky Security Service will be started or stopped.

Starting Kaspersky Embedded Systems Security for Windows components in the operating system safe mode

This section provides information about Kaspersky Embedded Systems Security for Windows working in the operating system safe mode.

About Kaspersky Embedded Systems Security for Windows working in the operating system safe mode

Kaspersky Embedded Systems Security for Windows components can be started when the operating system loads in safe mode. In addition to the Kaspersky Security Service (kavfs.exe), the klam.sys driver is loaded. It is used to register the Kaspersky Security Service as a protected service during the start of the operating system. For more details, see section Registering the Kaspersky Security Service as a protected service.

Kaspersky Embedded Systems Security for Windows can be started in the following safe modes of the operating system:

- Safe Mode Minimal – This mode is started when the standard option of the operating system safe mode is selected. At that, Kaspersky Embedded Systems Security for Windows can start the following components:
  - Real-Time File Protection.
  - On-Demand Scan.
  - Applications Launch Control and Rule Generator for Applications Launch Control.
  - Log Inspection.
  - File Integrity Monitor.
  - Baseline File Integrity Monitor.
  - Application Integrity Control.

Safe Mode with Networking – In this mode, the operating system is loaded in safe mode with network drivers. In addition to the components started in Safe Mode Minimal, Kaspersky Embedded Systems Security for Windows can start the following components in this mode:

- Database Update.
- Software Modules Update.

Starting Kaspersky Embedded Systems Security for Windows in safe mode

By default, Kaspersky Embedded Systems Security for Windows is not started when the operating system is loaded in safe mode.

To make Kaspersky Embedded Systems Security for Windows start in the operating system safe mode:

1. Start Windows Registry Editor (C:\Windows\regedit.exe).
2. Open the [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters] key of the system registry.
3. Open the LoadInSafeMode parameter.
4. Set the value to `1`.

5. Click the **OK** button.

To cancel start of Kaspersky Embedded Systems Security for Windows in the operating system safe mode:

1. Start Windows Registry Editor (C:\Windows\regedit.exe).
2. Open the [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters] key of the system registry.
3. Open the LoadInSafeMode parameter.
4. Set the value to `0`.
5. Click the **OK** button.

Kaspersky Embedded Systems Security for Windows self-defense

This section provides information about Kaspersky Embedded Systems Security for Windows self-defense mechanisms.

About Kaspersky Embedded Systems Security for Windows self-defense

Kaspersky Embedded Systems Security for Windows has self-defense mechanisms that protect the application against modification or deletion of its folders, memory processes, and system registry entries.

Protection from changes to folders with installed Kaspersky Embedded Systems Security for Windows components

Kaspersky Embedded Systems Security for Windows blocks renaming and deletion of folders with the installed application components by any user account. By default, the paths to the application installation folders are as follows:

- For the 32-bit version of Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security for Windows\
- On the 64-bit version of Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security for Windows\

Protection from changes to Kaspersky Embedded Systems Security for Windows registry keys

Kaspersky Embedded Systems Security for Windows restricts access to the following registry branches and keys, which facilitates loading of application drivers and services:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfs]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsgt]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsslp]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klelaml]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klfltdev]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klramdisk]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.4\CrashDump]

- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.4] (on Microsoft Windows 64-bit)
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.4\Trace]

The rights to change these registry branches and keys are granted to Local System (SYSTEM) account only. User and Administrator accounts are granted read-only rights.

Protection from changes to the memory of program service parts

To protect program service parts from third-party processes, Kaspersky Embedded Systems Security for Windows drivers restrict access to the following executable files:

- kavfs.exe
- kavfswp.exe
- kavfswh.exe
- kavfsgt.exe

By default, access to the memory of Kaspersky Embedded Systems Security for Windows service parts is restricted for third-party processes.

You can enable the self-defense functions in the policy properties of Kaspersky Embedded Systems Security for Windows Console and Kaspersky Embedded Systems Security for Windows Administration Plug-in.

Registering Kaspersky Security as a protected service

Protected Process Light ("PPL") technology ensures that the operating system only loads trusted services and processes. To start a service as a protected service, the *Early Launch Antimalware* driver must be installed on the protected device.

An *Early Launch Antimalware* (also referred to as "ELAM") driver provides protection for the devices in your network when they start and before third-party drivers are initialized.

An ELAM driver is automatically installed during Kaspersky Embedded Systems Security for Windows installation and is used for registering the Kaspersky Security Service as a PPL when the operating system starts. When the Kaspersky Security Service (KAVFS) is started as a system protected process, other non-protected processes on the system are not able to inject threads, write into the virtual memory of the protected process, or stop the service.

When a process is started as a PPL, it cannot be managed by a user regardless of the assigned user permissions. The Kaspersky Security Service registration as PPL using the ELAM driver is supported on the Microsoft Windows 10 and higher operating systems. If you install Kaspersky Embedded Systems Security for Windows on a server running an operating system that supports PPL, permission management will not be available for the Kaspersky Security Service (KAVFS).

To install Kaspersky Embedded Systems Security for Windows as a PPL:

```
msiexec /i ess_x64.msi NOPPL=0 EULA=1 PRIVACYPOLICY=1 /qn
```

Where the `NOPPL` option indicates registering the Kaspersky Security service as a protected process. Possible option values:

- `0`: Kaspersky Security service is registered in the operating system as a protected process.
- `1`: Kaspersky Security service is not registered in the operating system as a protected process.

Managing access permissions for Kaspersky Embedded Systems Security for Windows functions

This section contains information about permissions to manage Kaspersky Embedded Systems Security for Windows and operating system services registered by the application, and instructions on how to configure these permissions.

About permissions to manage Kaspersky Embedded Systems Security for Windows

By default, access to all Kaspersky Embedded Systems Security for Windows functions is granted to users in the "Administrators" group on the protected device, users in the ESS Administrators group created on the protected device during installation of Kaspersky Embedded Systems Security for Windows, and the SYSTEM group.

Users who have Edit permissions access level for Kaspersky Embedded Systems Security for Windows can grant access to Kaspersky Embedded Systems Security for Windows functions to other users registered on the protected device or included in the domain.

Users who are not registered in the list of Kaspersky Embedded Systems Security for Windows users cannot open the Application Console.

You can choose one of the following preset access levels for a user or group of users:

- **Full control** – access to all application functions: the ability to view and edit Kaspersky Embedded Systems Security for Windows general settings, component settings, and Kaspersky Embedded Systems Security for Windows user permissions; and the ability to view Kaspersky Embedded Systems Security for Windows statistics.
- **Modification** – access to all application functions except editing of user permissions: the ability to view and edit Kaspersky Embedded Systems Security for Windows general settings and Kaspersky Embedded Systems Security for Windows component settings.
- **Read** – the ability to view Kaspersky Embedded Systems Security for Windows general settings, Kaspersky Embedded Systems Security for Windows component settings, Kaspersky Embedded Systems Security for Windows statistics, and Kaspersky Embedded Systems Security for Windows user permissions.

You can also configure advanced access permissions: allow or block access to specific functions of Kaspersky Embedded Systems Security for Windows.

If you have manually configured access permissions for a user or group, then the **Special permissions** access level is set for this user or group.

About access permissions for Kaspersky Embedded Systems Security for Windows functions

User rights	Description
Task management	Ability to start / stop / pause / resume Kaspersky Embedded Systems Security for Windows tasks.
Create and delete On-Demand Scan tasks	Ability to create and delete On-Demand Scan tasks.
Edit settings	Ability to: • Import Kaspersky Embedded Systems Security for Windows settings from a configuration file. • Edit the application settings.
Read settings	Ability to: • View Kaspersky Embedded Systems Security for Windows general settings and task settings. • Export Kaspersky Embedded Systems Security for Windows settings to a configuration file. • View settings for task logs, system audit log, and notifications.
Manage storages	Ability to: • Move objects to Quarantine. • Remove objects from Quarantine and Backup. • Restore objects from Quarantine and Backup.
Manage logs	Ability to delete task logs and clear the system audit log.
Read logs	Ability to view Anti-Virus events in task logs and the system audit log.
Read statistics	Ability to view statistics for each Kaspersky Embedded Systems Security for Windows task.
Application licensing	Ability to activate Kaspersky Embedded Systems Security for Windows.
Uninstalling the application	Ability to uninstall Kaspersky Embedded Systems Security for Windows.
Read permissions	Ability to view the list of Kaspersky Embedded Systems Security for Windows users and user access privileges.
Edit permissions	Ability to: • Edit the list of users with access to application management. • Edit user access permissions for Kaspersky Embedded Systems Security for Windows functions.

About permissions to manage registered services

During installation, Kaspersky Embedded Systems Security for Windows registers in Windows the Kaspersky Security Service (KAVFS), the Kaspersky Security Management Service (KAVFSGT) and Kaspersky Security Exploit Prevention Service (KAVFSSLP).

The Kaspersky Security Service can be registered as a Protected Process Light using the ELAM driver on Microsoft Windows 10 and higher operating systems. When a process is started as a PPL, it cannot be managed by a user regardless of the assigned user permissions. If you install Kaspersky Embedded Systems Security for Windows on a protected device running an operating system that supports PPL, permission management will not be available for the Kaspersky Security Service (KAVFS).

Kaspersky Security Service

By default, access permissions for managing the Kaspersky Security Service are granted to users in the Administrators group on the protected device, as well as to the SERVICE and INTERACTIVE groups with read permissions and to the SYSTEM group with read and execute permissions.

Users who have the Edit permissions level access can grant access permissions for managing Kaspersky Security Service to other users registered on the protected device or included in the domain.

Kaspersky Security Management Service

To manage the application via the Application Console installed on a different protected device, the account whose permissions are used to connect to Kaspersky Embedded Systems Security for Windows must have full access to the Kaspersky Security Management Service on the protected device.

By default, access to the Kaspersky Security Management Service is granted to users in the "Administrators" group on the protected device and users in the ESS Administrators group created on the protected device during installation of Kaspersky Embedded Systems Security for Windows.

You can only manage the Kaspersky Security Management Service via the Microsoft Windows Services snap-in.

Kaspersky Security Exploit Prevention Service

By default, access permissions for managing the Kaspersky Security Exploit Prevention Service are granted to users in the Administrators group on the protected device, as well as to the SYSTEM group with read and execute permissions.

About access permissions for the Kaspersky Security Management Service

You can review the list of Kaspersky Embedded Systems Security for Windows services.

During installation, Kaspersky Embedded Systems Security for Windows registers the Kaspersky Security Management Service (KAVFSGT). To manage the application via the Application Console installed on a different protected device, the account used to connect to Kaspersky Embedded Systems Security for Windows must have full access to the Kaspersky Security Management Service on the protected device.

By default, access to the Kaspersky Security Management Service is granted to users in the "Administrators" group on the protected device and users in the ESS Administrators group created on the protected device during installation of Kaspersky Embedded Systems Security for Windows.

You can only manage the Kaspersky Security Management Service via the Microsoft Windows Services snap-in.

You cannot allow or block user access to the Kaspersky Security Management Service by configuring Kaspersky Embedded Systems Security for Windows.

You can connect to Kaspersky Embedded Systems Security for Windows from a local account if an account with the same user name and password is registered on the protected device.

About permissions to manage the Kaspersky Security Service

During installation, Kaspersky Embedded Systems Security for Windows registers the Kaspersky Security Service (KAVFS) in Windows, and internally enables the functional components that are started at operating system startup. To reduce the risk of third-party access to application functions and security settings on the protected device via the Kaspersky Security Service, you can restrict permissions for managing the Kaspersky Security Service from the Application Console or the Administration Plug-in.

By default, access permissions for managing the Kaspersky Security Service are granted to users in the Administrators group on the protected device. Read permissions are granted to the SERVICE and INTERACTIVE groups, and read and execute permissions are granted to the SYSTEM group.

You cannot delete the SYSTEM user account or edit permissions for this account. If the permissions for the SYSTEM account are edited, the maximum privileges are restored for this account when you save the changes.

Users who have access to functions of the Edit permissions level can grant access permissions for managing the Kaspersky Security Service to other users registered on the protected device or included in the domain.

You can choose one of the following preset levels of access permissions for a user or group of users of Kaspersky Embedded Systems Security for Windows for managing the Kaspersky Security Service:

- **Full control**: ability to view and edit general settings and user permissions for the Kaspersky Security Service, and to start and stop the Kaspersky Security Service.
- **Read**: ability to view Kaspersky Security Service general settings and user permissions.
- **Modification**: ability to view and edit Kaspersky Security Service general settings and user permissions.
- **Execution**: ability to start and stop the Kaspersky Security Service.

You can also configure advanced access permissions: allow or deny access to specific Kaspersky Embedded Systems Security for Windows functions (see the table below).

If you have manually configured access permissions for a user or group, then the **Special permissions** access level is set for this user or group.

Access permissions for Kaspersky Security Service functions

Feature	Description
View service configurations	Ability to view Kaspersky Security Service general settings and user permissions.

Request service status from Service Control Manager	Ability to request the execution status of the Kaspersky Security Service from the Microsoft Windows Service Control Manager.
Request status from service	Ability to request the service execution status from the Kaspersky Security Service.
Read list of dependent services	Ability to view a list of services which the Kaspersky Security Service depends on and which depend on the Kaspersky Security Service.
Editing service settings	Ability to view and edit Kaspersky Security Service general settings and user permissions.
Start the service	Ability to start the Kaspersky Security Service.
Stop the service	Ability to stop the Kaspersky Security Service.
Pause / Resume the service	Ability to pause and resume the Kaspersky Security Service.
Read permissions	Ability to view the list of Kaspersky Security Service users and each user's access privileges.
Edit permissions	Ability to: • Add and remove Kaspersky Security Service users. • Edit user access permissions for the Kaspersky Security Service.
Delete the service	Ability to unregister the Kaspersky Security Service in the Microsoft Windows Service Control Manager.
User defined requests to service	Ability to create and send user requests to the Kaspersky Security Service.

Managing access permissions via the Administration Plug-in

In this section, learn how to navigate the Administration Plug-In interface and configure access permissions for one or all protected devices on the network.

Configuring access permissions for Kaspersky Embedded Systems Security for Windows and the Kaspersky Security Service

You can edit the list of users and user groups allowed to access Kaspersky Embedded Systems Security for Windows functions and manage the Kaspersky Security Service. You can also edit the access permissions of those users and user groups.

To add or remove a user or group from the list:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:

- To configure application settings for a group of protected devices, select the **Policies** tab and open the **Properties: <Policy name>** window.

- To configure the settings of a task or application for an individual protected device, select the **Devices** tab and go to local task settings or application settings.

4. In the **Supplementary** section, perform one of the following steps:

   - Click the **Settings** button in the **User access permissions for application management** subsection if you want to edit the list of users who have access permissions for managing Kaspersky Embedded Systems Security for Windows functions.

   - Click the **Settings** button in the **User access permissions for Kaspersky Security Service management** subsection if you want to edit the list of users who have access permissions for managing the Kaspersky Security Service.

     The **Permissions for Kaspersky Embedded Systems Security 3.4 for Windows** window opens.

5. In the window that opens, perform the following operations:

   - In order to add a user or group to the list, click the **Add** button and select the user or group that you want to grant privileges to.

   - To remove a user or group from the list, select the user or group whose access you want to restrict, and click the **Remove** button.

6. Click the **Apply** button.

The selected users (groups) are added or removed.

To edit the permissions of a user or group to manage Kaspersky Embedded Systems Security for Windows or the Kaspersky Security Service:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.

2. Select the administration group for which you want to configure application settings.

3. Perform one of the following actions in the details pane of the selected administration group:

   - To configure application settings for a group of protected devices, select the **Policies** tab and open the **Properties: <Policy name>** window.

   - To configure the settings of a task or application for an individual protected device, select the **Devices** tab and go to local task settings or application settings.

4. In the **Supplementary** section, perform one of the following steps:

   - Click the **Settings** button in the **User access permissions for application management** subsection if you want to edit the list of users who have access permissions for managing Kaspersky Embedded Systems Security for Windows functions.

   - Click the **Settings** button in the **User access permissions for Kaspersky Security Service management** subsection if you want to edit the list of users who have access permissions for managing the application via the Kaspersky Security Service.

     The **Permissions for Kaspersky Embedded Systems Security for Windows** window opens.

5. In the window that opens, in the **Group or user names** list, select the user or group of users whose permissions you want to change.

6. In the **Permissions for <User (Group)>** section, select the **Allow** or **Deny** check boxes for the following access levels:

   - **Full control**: full set of permissions to manage Kaspersky Embedded Systems Security for Windows or the Kaspersky Security Service.

   - **Read**:

     - The following permissions to manage Kaspersky Embedded Systems Security for Windows: **Retrieve statistics**, **Read settings**, **Read logs** and **Read permissions**.

     - The following permissions to manage the Kaspersky Security Service: **Read service settings**, **Request status from Service Control Manager**, **Request status from service**, **Read list of dependent services**, **Read permissions**.

   - **Modification**:

     - All permissions to manage Kaspersky Embedded Systems Security for Windows, except **Edit permissions**.

     - The following permissions to manage the Kaspersky Security Service: **Modify service settings**, **Read permissions**.

   - **Special permissions**: the following permissions to manage the Kaspersky Security Service: **Starting service**, **Stop service**, **Pause / Resume service**, **Read permissions**, **User defined requests to service**.

7. To configure advanced permissions for a user or group (**Special permissions**), click the **Advanced** button.

   a. In the **Advanced security settings for Kaspersky Embedded Systems Security for Windows** window that opens, select the desired user or group.

   b. Click the **Edit** button.

   c. In the drop-down list in the top part of the window, select the type of access control (**Allow** or **Block**).

   d. Select the check boxes next to the functions that you want to allow or block for the selected user or group.

   e. Click the **OK** button.

   f. In the **Advanced security settings for Kaspersky Embedded Systems Security for Windows** window, click **OK**.

8. In the **Permissions for Kaspersky Embedded Systems Security for Windows** window, click the **Apply** button.

The configured permissions for managing Kaspersky Embedded Systems Security for Windows or the Kaspersky Security Service are saved.

Password-protected access to Kaspersky Embedded Systems Security for Windows functions

You can restrict access to application management and registered services by configuring user permissions. You can also set password protection in the Kaspersky Embedded Systems Security for Windows settings for additional protection of critical operations.

Kaspersky Embedded Systems Security for Windows requests a password when you attempt to access the following application functions:

- connect to the Application Console;
- uninstall Kaspersky Embedded Systems Security for Windows;
- modify Kaspersky Embedded Systems Security for Windows components;
- execute command-line commands.

The Kaspersky Embedded Systems Security for Windows interface disguises the specified password on screen. Kaspersky Embedded Systems Security for Windows stores the password as a checksum calculated when the password is entered.

Kaspersky Embedded Systems Security for Windows doesn't check password strength and doesn't block password entry after a number of failed attempts.

When creating a password, you are recommended to meet the following conditions:

- The password doesn't contain the account name or computer name.
- The password is at least 8 characters long.
- The password contains characters that match at least three of the following categories:
  - uppercase latin letters (A-Z);
  - lowercase latin letters (a-z);
  - numbers (0-9);
  - symbols of exclamation point (!), dollar sign ($), pound sign (#) and percent sign (%).

You can export and import a password-protected application configuration. A configuration file created by exporting a protected application configuration contains the password checksum and the value of the modifier used to pad the password string.

Do not change the checksum or modifier in the configuration file. Importing a password-protected configuration that has been changed manually may cause access to the application to be entirely blocked.

To protect access to Kaspersky Embedded Systems Security for Windows functions:

1. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node. Select the administration group with the protected devices whose application settings you want to configure.
2. Perform one of the following actions in the details pane of the selected administration group:
   - To configure policy settings for a group of protected devices, select the **Policies** tab and open the properties of the **<Policy name>** by means of the context menu.

- If you want to configure application settings for a single protected device, open the required settings in the **Application settings** window in the Kaspersky Security Center.

3. In the **Application settings** section of the **Security and reliability** tab, click the **Settings** button.

   The **Security settings** window opens.

4. In the **Password protection settings** section, select the **Apply password protection** check box.

   The **Password** and **Confirm password** fields become active.

5. In the **Password** field, enter the password you want to use to protect access to Kaspersky Embedded Systems Security for Windows functions.

6. In the **Confirm password** field, enter the password again.

7. Click the **OK** button.

The specified settings are saved. Kaspersky Embedded Systems Security for Windows will request the specified password to access protected functions.

This password cannot be recovered. Losing your password will result in the complete loss of control of the application. Additionally, it will be impossible to uninstall the application from the protected device.

You can reset the password at any time. To do that, clear the **Apply password protection** check box and save changes. Password protection will be disabled and the old password checksum will be removed. Repeat the password creation process with a new password.

Managing access permissions via the Application Console

In this section, learn how to navigate the Application Console interface and configure access permissions on a protected device.

Configuring access permissions for managing Kaspersky Embedded Systems Security for Windows and the Kaspersky Security Service

You can edit the list of users and user groups allowed to access Kaspersky Embedded Systems Security for Windows functions and manage the Kaspersky Security Service. You can also edit the access permissions of those users and user groups.

To add or remove a user or group from the list:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.

2. Select the administration group for which you want to configure application settings.

3. Perform one of the following actions in the details pane of the selected administration group:

   - To configure application settings for a group of protected devices, select the **Policies** tab and open the **Properties: <Policy name>** window.

- To configure the settings of a task or application for an individual protected device, select the **Devices** tab and go to local task settings or application settings.

4. In the **Supplementary** section, perform one of the following steps:

   - Click the **Settings** button in the **User access permissions for application management** subsection if you want to edit the list of users who have access permissions for managing Kaspersky Embedded Systems Security for Windows functions.

   - Click the **Settings** button in the **User access permissions for Kaspersky Security Service management** subsection if you want to edit the list of users who have access permissions for managing the Kaspersky Security Service.

     The **Permissions for Kaspersky Embedded Systems Security 3.4 for Windows** window opens.

5. In the window that opens, perform the following operations:

   - In order to add a user or group to the list, click the **Add** button and select the user or group that you want to grant privileges to.

   - To remove a user or group from the list, select the user or group whose access you want to restrict, and click the **Remove** button.

6. Click the **Apply** button.

The selected users (groups) are added or removed.

To edit the permissions of a user or group to manage Kaspersky Embedded Systems Security for Windows or the Kaspersky Security Service:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.

2. Select the administration group for which you want to configure application settings.

3. Perform one of the following actions in the details pane of the selected administration group:

   - To configure application settings for a group of protected devices, select the **Policies** tab and open the **Properties: <Policy name>** window.

   - To configure the settings of a task or application for an individual protected device, select the **Devices** tab and go to local task settings or application settings.

4. In the **Supplementary** section, perform one of the following steps:

   - Click the **Settings** button in the **User access permissions for application management** subsection if you want to edit the list of users who have access permissions for managing Kaspersky Embedded Systems Security for Windows functions.

   - Click the **Settings** button in the **User access permissions for Kaspersky Security Service management** subsection if you want to edit the list of users who have access permissions for managing the application via the Kaspersky Security Service.

     The **Permissions for Kaspersky Embedded Systems Security for Windows** window opens.

5. In the window that opens, in the **Group or user names** list, select the user or group of users whose permissions you want to change.

6. In the **Permissions for <User (Group)>** section, select the **Allow** or **Deny** check boxes for the following access levels:

   - **Full control**: full set of permissions to manage Kaspersky Embedded Systems Security for Windows or the Kaspersky Security Service.
   - **Read**:
     - The following permissions to manage Kaspersky Embedded Systems Security for Windows: **Retrieve statistics**, **Read settings**, **Read logs** and **Read permissions**.
     - The following permissions to manage the Kaspersky Security Service: **Read service settings**, **Request status from Service Control Manager**, **Request status from service**, **Read list of dependent services**, **Read permissions**.
   - **Modification**:
     - All permissions to manage Kaspersky Embedded Systems Security for Windows, except **Edit permissions**.
     - The following permissions to manage the Kaspersky Security Service: **Modify service settings**, **Read permissions**.
   - **Special permissions**: the following permissions to manage the Kaspersky Security Service: **Starting service**, **Stop service**, **Pause / Resume service**, **Read permissions**, **User defined requests to service**.

7. To configure advanced permissions for a user or group (**Special permissions**), click the **Advanced** button.

   a. In the **Advanced security settings for Kaspersky Embedded Systems Security for Windows** window that opens, select the desired user or group.

   b. Click the **Edit** button.

   c. In the drop-down list in the top part of the window, select the type of access control (**Allow** or **Block**).

   d. Select the check boxes next to the functions that you want to allow or block for the selected user or group.

   e. Click the **OK** button.

   f. In the **Advanced security settings for Kaspersky Embedded Systems Security for Windows** window, click **OK**.

8. In the **Permissions for Kaspersky Embedded Systems Security for Windows** window, click the **Apply** button.

9. The configured permissions for managing Kaspersky Embedded Systems Security for Windows or the Kaspersky Security Service are saved.

Password-protected access to Kaspersky Embedded Systems Security for Windows functions

You can restrict access to application management and registered services by configuring user permissions. You can also set password protection in the Kaspersky Embedded Systems Security for Windows settings for additional protection of critical operations.

Kaspersky Embedded Systems Security for Windows requests a password when you attempt to access the following application functions:

- connect to the Application Console;
- uninstall Kaspersky Embedded Systems Security for Windows;
- modify Kaspersky Embedded Systems Security for Windows components;
- execute command-line commands.

The Kaspersky Embedded Systems Security for Windows interface disguises the specified password on screen. Kaspersky Embedded Systems Security for Windows stores the password as a checksum calculated when the password is entered.

Kaspersky Embedded Systems Security for Windows doesn't check password strength and doesn't block password entry after a number of failed attempts.

When creating a password, you are recommended to meet the following conditions:

- The password doesn't contain the account name or computer name.
- The password is at least 8 characters long.
- The password contains characters that match at least three of the following categories:
  - uppercase latin letters (A-Z);
  - lowercase latin letters (a-z);
  - numbers (0-9);
  - symbols of exclamation point (!), dollar sign ($), pound sign (#) and percent sign (%).

You can export and import a password-protected application configuration. A configuration file created by exporting a protected application configuration contains the password checksum and the value of the modifier used to pad the password string.

Do not change the checksum or modifier in the configuration file. Importing a password-protected configuration that has been changed manually may cause access to the application to be entirely blocked.

To protect access to Kaspersky Embedded Systems Security for Windows functions:

1. In the Application Console tree, select the **Kaspersky Embedded Systems Security for Windows** node and do one of the following:
   - Click the **Application properties** link in the details pane of the node.
   - Select **Properties** in the node's context menu.

   The **Application settings** window is displayed.

2. On the **Security and reliability** tab in the **Password protection settings** section, select the **Apply password protection** check box.

   The **Password** and **Confirm password** fields become active.

3. In the **Password** field, enter the password you want to use to protect access to Kaspersky Embedded Systems Security for Windows functions.

4. In the **Confirm password** field, enter the password again.

5. Click the **OK** button.

This password cannot be recovered. Losing your password results in complete loss of control of the application. Additionally, it will be impossible to uninstall the application from the protected device.

You can reset the password at any time. To do that, clear the **Apply password protection** check box and save changes. Password protection will be disabled and the old password checksum will be removed. Repeat the password creation process with a new password.

Managing access permissions via the Web Plug-in

In this section, learn how to navigate the Web Plug-In interface and configure access permissions for one or all protected devices on the network.

Configuring access permissions for Kaspersky Embedded Systems Security for Windows and the Kaspersky Security Service

To configure the access permissions for a user or group you need to specify the security descriptor string using the security descriptor definition language (SDDL). For detailed information about the security descriptor string, please visit the Microsoft website.

To configure the access permissions for a user or group:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.

2. Click the policy name you want to configure.

3. In the **<Policy name>** window that opens, select the **Application settings** tab.

4. Select the **Supplementary** section.

5. Do one of the following:

   - Click the **Settings** button in the **User access permissions for application management** subsection if you want to edit the list of users who have access permissions for managing Kaspersky Embedded Systems Security for Windows functions.

   - Click the **Settings** button in the **User access permissions for Kaspersky Security Service management** subsection if you want to edit the list of users who have access permissions for managing the Kaspersky Security Service.

6. Add a user or group by specifying the security descriptor string in the **User access permissions for application management** or **User access permissions for Kaspersky Security Service management** window.

7. Click the **OK** button.

Password-protected access to Kaspersky Embedded Systems Security for Windows functions

You can restrict access to application management and registered services by configuring user permissions. You can also set password protection in the Kaspersky Embedded Systems Security for Windows settings for additional protection of critical operations.

Kaspersky Embedded Systems Security for Windows requests a password when you attempt to access the following application functions:

- connect to the Application Console;
- uninstall Kaspersky Embedded Systems Security for Windows;
- modify Kaspersky Embedded Systems Security for Windows components;
- execute command-line commands.

The Kaspersky Embedded Systems Security for Windows interface disguises the specified password on screen. Kaspersky Embedded Systems Security for Windows stores the password as a checksum calculated when the password is entered.

Kaspersky Embedded Systems Security for Windows doesn't check password strength and doesn't block password entry after a number of failed attempts.

When creating a password, you are recommended to meet the following conditions:

- The password doesn't contain the account name or computer name.
- The password is at least 8 characters long.
- The password contains characters that match at least three of the following categories:
  - uppercase latin letters (A-Z);
  - lowercase latin letters (a-z);
  - numbers (0-9);
  - symbols of exclamation point (!), dollar sign ($), pound sign (#) and percent sign (%).

You can export and import a password-protected application configuration. A configuration file created by exporting a protected application configuration contains the password checksum and the value of the modifier used to pad the password string.

Do not change the checksum or modifier in the configuration file. Importing a password-protected configuration that has been changed manually may cause access to the application to be entirely blocked.

To protect access to Kaspersky Embedded Systems Security for Windows functions:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.
2. Click the policy name you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.
4. Select the **Application settings** section.
5. In the **Security and reliability** section, click the **Settings** button.
6. In the **Password protection settings** section, select the **Apply password protection** check box.
7. In the **Password** field, enter the password you want to use to protect access to Kaspersky Embedded Systems Security for Windows functions.
8. Click the **OK** button.

The specified settings are saved. Kaspersky Embedded Systems Security for Windows will request the specified password to access protected functions.

This password cannot be recovered. Losing your password will result in the complete loss of control of the application. Additionally, it will be impossible to uninstall the application from the protected device.

You can reset the password at any time. To do that, clear the **Apply password protection** check box and save changes. Password protection will be disabled and the old password checksum will be removed. Repeat the password creation process with a new password.

Real-Time File Protection

This section contains information about the Real-Time File Protection task and how to configure it.

About the Real-Time File Protection task

When the Real-Time File Protection task is running, Kaspersky Embedded Systems Security for Windows scans the following protected device objects when they are accessed:

- Operating system objects.
- NTFS alternate data streams.
- Master boot records and boot sectors on local hard drives and external devices.

When any application writes or reads a file on the protected device, Kaspersky Embedded Systems Security for Windows intercepts the file, scans it for threats, and, if a threat is detected, performs a default action or an action you have specified: try to disinfect, move to Quarantine, or delete it. Before disinfection or deletion, Kaspersky Embedded Systems Security for Windows saves an encrypted copy of the source file to the Backup folder.

Kaspersky Embedded Systems Security for Windows also detects malware for processes running under Windows Subsystem for Linux®. For such processes, the Real-Time File Protection task applies action defined by the current configuration.

About the task protection scope and security settings

By default, the Real-Time File Protection task protects all objects of the device file system. If there is no security requirement to protect all objects of the file system or you want to exclude any objects from the task scope, you can limit the protection scope.

In the Application Console, the protection scope is displayed as a tree or list of the device's file resources that Kaspersky Embedded Systems Security for Windows can monitor. By default, the network file resources of the device are displayed as a list.

In the Administration Plug-in only the list view is available.

To display network file resources as a tree in the Application Console,

open the drop-down list in the upper left section of the **Protection scope settings** window and select **Tree-view**.

Whether the protected device's file resources are displayed as a list or a tree, the node icons have the following meanings:

☑ The node is included in the protection scope.

☐ The node is excluded from the protection scope.

☑ At least one of this node's child nodes is excluded from the protection scope, or the security settings of the child node(s) differ(s) from those of the parent node (for the tree view only).

The icon is displayed if all child nodes are selected, but the parent node is not selected. In this case, changes in the composition of the parent node's files and folders are disregarded automatically when the protection scope for the selected child node is created.

Using the Application Console, you can also add virtual drives to the protection scope. The names of the virtual nodes are displayed in blue.

Security settings

The task security settings can be configured as common settings for all nodes or items included in the protection scope, or as different settings for each node or item in the device's file resource tree or list.

Security settings configured for the selected parent node are automatically applied to all its child nodes. The security settings of the parent node are not applied to child nodes that are configured separately.

The settings for a selected protection scope can be configured using one of the following methods:

- Selecting one of three predefined security levels.
- Configuring the security settings manually for the selected nodes or items in the file resource tree or list (the security level changes to **Custom**).

A set of settings for a node or item can be saved in a template in order to be applied later to other nodes or items.

About virtual protection scopes

Kaspersky Embedded Systems Security for Windows can scan not only existing folders and files on hard drives and removable drives, but also drives that are dynamically created on the protected device by various applications and services.

If all device objects are included in the protection scope, these dynamic nodes will automatically be included in the protection scope. However, if you want to specify special values for the security settings of these dynamic nodes or if you have selected only part of the device for protection, then in order to include virtual drives, files or folders in the protection scope, you will first have to create them in the Application Console: that is, specify the virtual protection scope. The drives, files and folders created will exist only in the Application Console, but not in the file structure of the protected device.

If, while creating a protection scope, all subfolders or files are selected without the parent folder being selected, then all virtual folders or files that appear in it will not automatically be included in the protected scope. "Virtual copies" of these should be created in the Application Console and added to the protection scope.

Predefined protection scopes

The file resource tree or list displays the nodes to which you have read-access based on the configured Microsoft Windows security settings.

Kaspersky Embedded Systems Security for Windows covers the following predefined protection scopes:

- **Local hard drives**. Kaspersky Embedded Systems Security for Windows protects files on the device hard drives.
- **Removable drives**. Kaspersky Embedded Systems Security for Windows protects files on external devices, such as CDs or removable drives. All removable drives, individual disks, folders or files can be included in or excluded from the protection scope.
- **Network**. Kaspersky Embedded Systems Security for Windows protects files that are written to network folders or read from them by applications running on the device. Kaspersky Embedded Systems Security for Windows does not protect files when such files are accessed by applications from other protected devices.
- **Virtual drives**. Virtual folders, files, and drives temporarily connected to the device can be included in the protection scope, for example, common cluster drives.

By default, you can view and configure predefined protection scopes in the scope list; you can also add predefined scopes to the list during its formation in the protection scope settings.

By default, the protection scope includes all predefined areas except virtual drives.

Virtual drives created using a SUBST command are not displayed in the protected device's file resource tree in the Application Console. To include objects on the virtual drive in the protection scope, include the device folder associated with the virtual drive in the protection scope.

Connected network drives will also not be displayed in the protected device's file resource list. To include objects on network drives in the protection scope, specify the path to the folder that corresponds to this network drive in UNC format.

About predefined security levels

One of the following predefined security levels for the nodes selected either in the protected device's file resource tree or file resource list can be applied: **Maximum performance**, **Recommended**, and **Maximum protection**. Each of these levels contains its own predefined set of security settings (see the table below).

Maximum performance

The **Maximum performance** security level is recommended if your network has additional protected device security measures, for example, firewalls and existing security policies, beyond using Kaspersky Embedded Systems Security for Windows on protected devices.

Recommended

The **Recommended** security level ensures the best combination of protection and performance impact on devices. Kaspersky experts recommend this level as adequate to protect devices on most corporate networks. The **Recommended** security level is set by default.

Maximum protection

The **Maximum protection** security level is recommended if your organization's network has elevated device security requirements.

Preset security levels and corresponding setting values

Options	Security level		
	Maximum performance	Recommended	Maximum protection
Objects protection	By extension	By format	By format
Protect only new and modified files	Enabled	Enabled	Disabled
Action to perform on infected and other objects	Block access and disinfect. Remove, if disinfection fails	Block access and perform action recommended by Kaspersky experts	Block access and disinfect. Remove, if disinfection fails
Action to perform on probably infected objects	Block access and quarantine	Block access and perform action recommended by Kaspersky experts	Block access and quarantine
System-critical objects are files required for the operation of the operating system and Kaspersky Embedded Systems Security for Windows. These files can not be deleted. Processes associated with such objects cannot be terminated.			
Exclude files	No	No	No
Do not detect	No	No	No
Stop scanning if it takes longer than (sec.)	60 sec.	60 sec.	60 sec.
Do not scan compound objects larger than (MB)	8 MB	8 MB	Not set
Scan alternate NTFS streams	Yes	Yes	Yes
Scan disk boot sectors and MBR	Yes	Yes	Yes
Compound objects protection	• Packed objects* * New and modified objects only	• SFX archives* • Packed objects* • Embedded OLE objects* * New and modified objects only	• SFX archives* • Packed objects* • Embedded OLE objects* * All objects
Entirely remove compound file that cannot be modified by the application in case of embedded object detection	No	No	Yes

The **Objects protection**, **Use iChecker technology**, **Use iSwift technology**, and **Use heuristic analyzer** settings are not included in the settings of the predefined security levels. If you edit the **Objects protection**, **Use iChecker technology**, **Use iSwift technology**, or **Use heuristic analyzer** security settings after selecting one of the predefined security levels, the security level that you have selected will not change.

File extensions scanned by default in the Real-Time File Protection task

Kaspersky Embedded Systems Security for Windows scans files with the following extensions by default:

- *386;*
- *acm;*
- *ade, adp;*
- *asp;*
- *asx;*
- *ax;*
- *bas;*
- *bat;*
- *bin;*
- *chm;*
- *cla, clas*;*
- *cmd;*
- *com;*
- *cpl;*
- *crt;*
- *dll;*
- *dpl;*
- *drv;*
- *dvb;*
- *dwg;*
- *efi;*
- *emf;*

- *eml;*
- *.exe*
- *fon;*
- *fpm;*
- *hlp;*
- *hta;*
- *htm, html*;*
- *htt;*
- *ico;*
- *inf;*
- *ini;*
- *ins;*
- *isp;*
- *jpg, jpe;*
- *js, jse;*
- *lnk;*
- *mbx;*
- *msc;*
- *msg;*
- *msi;*
- *msp;*
- *mst;*
- *nws;*
- *ocx;*
- *oft;*
- *otm;*
- *pcd;*
- *pdf;*

- *php;*
- *pht;*
- *phtm*;*
- *pif;*
- *plg;*
- *png;*
- *pot;*
- *prf;*
- *prg;*
- *reg;*
- *rsc;*
- *rtf;*
- *scf;*
- *scr;*
- *sct;*
- *shb;*
- *shs;*
- *sht;*
- *shtm*;*
- *swf;*
- *sys;*
- *the;*
- *them*;*
- *tsp;*
- *url;*
- *vb;*
- *vbe;*
- *vbs;*

- *vxd;*
- *wma;*
- *wmf;*
- *wmv;*
- *wsc;*
- *wsf;*
- *wsh;*
- *do?;*
- *md?;*
- *mp?;*
- *ov?;*
- *pp?;*
- *vs?;*
- *xl?.*

Default Real-Time File Protection task settings

By default, the Real-Time File Protection task uses the settings described in the table below. You can change the values of these settings.

Default Real-Time File Protection task settings

Setting	Default value	Description
Protection scope	The entire protected device, excluding virtual drives.	Use this option to change the protection scope.
Security settings	Common settings for the entire protection scope correspond to the **Recommended** security level.	For nodes selected in the protected device's file resource list or tree, you can: • Select a different predefined security level • Manually change security settings You can save a group of security settings for a selected node as a template to use later for a different node.
Objects protection mode	**Smart mode**	Use this option to select the protection mode, i.e. define the type of access attempts for which Kaspersky Embedded Systems Security for Windows scans objects.
Heuristic analyzer	The **Medium** security level is	The Heuristic Analyzer can be enabled or

	applied.	disabled and the analysis level can be configured.
Apply Trusted Zone	Applied.	General list of exclusions that can be used in selected tasks.
Use KSN for protection	Applied.	Use this option to improve your device's protection using the Kaspersky Security Network cloud service (available if the KSN Statement is accepted).
Task start schedule	At application start.	Use this option to configure for scheduled task start.
Block access to network shared resources for the sessions that show malicious activity	Not applied.	Use this option to block current session and to add host IP or host LUID for which malicious activity was detected in the Blocked hosts storage section.
Launch critical areas scan when active infection is detected	Applied.	When active infection is detected, Kaspersky Embedded Systems Security for Windows creates and launches a temporary Critical Areas Scan task.

Managing the Real-Time File Protection task via the Administration Plug-in

In this section, learn how to navigate the Administration Plug-In interface and configure task settings for one or all protected devices on the network.

Navigation

Learn how to navigate to the required task settings via the chosen interface.

Opening policy settings for the Real-Time File Protection task

To open the Real-Time File Protection task settings via the Kaspersky Security Center policy:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure the task.
3. Select the **Policies** tab.
4. Double-click the policy name you want to configure.
5. In the **Properties: <Policy name>** window that opens, select the **Real-Time Computer Protection** section.
6. Click **Settings** in the **Real-Time File Protection** subsection.

   The **Real-time file protection** window opens.

If a protected device is being managed by an active Kaspersky Security Center policy and this policy blocks changes to the application settings, these settings cannot be edited via the Application Console.

Opening the Real-Time File Protection task settings

To open the Real-Time File Protection task settings window for a single network device:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure the task.
3. Select the **Devices** tab.
4. Open the **Properties: <Protected device name>** window in one of the following ways:
   - Double-click the name of the protected device.
   - Open the context menu of the protected device name and select the **Properties** item.

   The **Properties: <Protected device name>** window opens.
5. In the **Tasks** section, select the **Real-Time File Protection** task.
6. Click the **Properties** button.
   The **Properties: Real-Time File Protection** window opens.

Configuring Real-Time File Protection task

To configure the Real-Time File Protection task settings:

1. Open the **Real-time file protection** window.
2. Configure the following task settings:
   - On the **General** tab:
     - Interception parameters
     - **Heuristic analyzer**
     - **Integration with other components**
   - On the **Task management** tab:
     - Task start schedule settings.
3. Select the **Protection scope** tab and do the following:
   - Click the **Add** or **Edit** button to edit the protection scope.

- In the window that opens, choose what you want to include in the task protection scope:
  - **Predefined scope**
  - **Disk, folder or network location**
  - **File**
- Select one of the predefined security levels or manually configure the protection settings.

4. Click the **OK** button in the **Real-time file protection** window.

Kaspersky Embedded Systems Security for Windows immediately applies the new settings to the running task. The date and time when the settings were modified and the values of task settings before and after modification are saved in the system audit log.

Selecting the protection mode

In the Real-Time File Protection task, the protection mode can be selected. The **Objects protection mode** section lets you specify the type of access attempts for which Kaspersky Embedded Systems Security for Windows scans objects.

The value of the **Objects protection mode** setting applies to the entire protection scope specified in the task. You cannot specify different values for the setting for individual nodes within the protection scope.

To select the protection mode:

1. Open the **Real-time file protection** window.
2. In the window that opens, open the **General** tab and select the protection mode that you want to set:
   - **Smart mode**
   - **On access and modification**
   - **On access**
   - **When run**
   - **Deeper analysis of launching processes (process launch is blocked until the analysis ends)**
3. Click the **OK** button.

The selected protection mode will take effect.

Configuring Heuristic Analyzer and integration with other application components

To start the KSN Usage task, you must accept the Kaspersky Security Network Statement.

To configure Heuristic Analyzer and integration with other components:

1. Open the **Real-time file protection** window.
2. On the **General** tab, clear or select the **Use heuristic analyzer** check box.
3. If necessary, adjust the level of analysis using the slider.
4. In the **Integration with other components** section, configure the following settings:
   - Select or clear the **Apply Trusted Zone** check box.
   - Select or clear the **Use KSN for protection** check box.

     The **Send data about scanned files** check box must be selected in the KSN Usage task settings.

   - Select or clear the **Block access to network shared resources for the sessions that show malicious activity** check box.
   - Select or clear the **Launch critical areas scan when active infection is detected** check box.
5. Click the **OK** button.

The configured task settings are applied immediately to a running task. If the task is not running, the modified settings are applied at next start.

Scheduling tasks

You can schedule local system and custom tasks in the Application Console. You cannot schedule group tasks in the Application Console.

To schedule group tasks using the Administration Plug-in:

1. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node.
2. Select the group that the protected device belongs to.
3. In the results pane, select the **Tasks** tab.
4. Open the **Properties: <Task name>** window in one of the following ways:
   - Double-click the name of the task.
   - Open the context menu of the task name and select the Properties item.
5. Select the **Schedule** section.
6. In the **Schedule settings** block, select the **Run by schedule** check box.

Fields with schedule settings for the On-Demand Scan and Update tasks are unavailable if scheduling of these tasks is blocked by a Kaspersky Security Center policy.

7. Configure schedule settings in accordance with your requirements. To do this, perform the following actions:

   a. in the **Frequency** list, select one of the following values:

   - **Hourly**, if you want the task to run at intervals of a specified number of hours; specify the number of hours in the **Every <number> hour(s)** field.
   - **Daily**, if you want the task to run at intervals of a specified number of days; specify the number of days in the **Every <number> day(s)** field.
   - **Weekly**, if you want the task to run at intervals of a specified number of weeks; specify the number of weeks in the **Every <number> week(s)** field. Specify the days of the week on which the task will be started (by default tasks run on Mondays).
   - **At application launch**, if you want the task to run every time Kaspersky Embedded Systems Security for Windows starts.
   - **After application database update**, if you want the task to run after every update of the application databases.

   b. Specify the time for the first task start in the **Start time** field.

   c. In the **Start date** field, specify the date when the schedule starts.

   After you have scheduled the start time, date and frequency of the task, the estimated time for the next start is displayed.

   Go to the **Schedule** tab and open the **Task settings** window. In the **Next start** field in the top of the window, the estimated start time is displayed. Each time you open the window, this estimated start time is updated and displayed.

   The **Next start** field displays the **Blocked by policy** value if Kaspersky Security Center active policy settings prohibit scheduled local system tasks from starting.

8. Use the **Advanced** tab to configure the following schedule settings in accordance with your requirements.

   - In the **Task stop settings** section:

     a. Select the **Duration** check box and, in the fields to the right, enter the maximum number of hours and minutes of task execution.

     b. Select the **Pause from** check box and, in the fields to the right, enter the start and end values of a time interval under 24 hours during which task execution will be paused.

   - In the **Advanced settings** block:

     a. Select the **Cancel schedule from** check box and specify the date from which the schedule will cease to apply.

     b. Select the **Run skipped tasks** check box to enable the start of skipped tasks.

c. Select the **Randomize the task start time within the interval of** check box and specify a value in minutes.

9. Click the **OK** button.

10. Click the **Apply** button to save the task start settings.

If you want to configure application settings for a single task using Kaspersky Security Center, see section "Configuring local tasks in the Application settings window of the Kaspersky Security Center".

Creating and configuring the task protection scope

To create and configure the task protection scope via the Kaspersky Security Center:

1. Open the **Real-time file protection** window.

2. Select the **Protection scope** tab.

   All items already protected by the task are listed in the **Protection scope** table.

3. Click the **Add** button to add new item to the list.

   The **Add objects to protection scope** window opens.

4. Select an object type to add it to a protection scope:

   - **Predefined scope** - to include one of the predefined scopes in the protection scope on the device. Then in the drop-down list, select the desired protection scope.
   - **Disk, folder or network location** - to include individual drive, folder or a network object in the protection scope. Then select the desired protection scope by clicking the **Browse** button.
   - **File** - to include an individual file in the protection scope. Then select the desired protection scope by clicking the **Browse** button.

   You cannot add an object to a protection scope if it has already been added as an exclusion from a protection scope.

5. To exclude individual items from the protection scope, clear check boxes next to the names of these items or take the following steps:

   a. Open the context menu of the protection scope by right-clicking it.

   b. In the context menu, select the **Add exclusion** option.

   c. In the **Add exclusion** window, select an object type that you want to add as an exclusion from the protection scope following the procedure used when adding an object to the protection scope.

6. To modify the protection scope or an existing exclusion, select the **Edit scope** option in the context menu of the desired protection scope.

7. To hide a previously added protection scope or an exclusion in the list of network file resources, select the **Remove scope** option in the context menu of the desired protection scope.

   A protection scope is removed from the Real-Time File Protection task scope when it is removed from the network file resource list.

8. Click the **OK** button.

The Protection scope settings window closes. The specified settings are saved.

The **Real-Time File Protection** task can be started if at least one of the device's file resource nodes is included in a protection scope.

Selecting predefined security levels for On-Demand Scan tasks

You can apply one of the following three predefined security levels to a node selected in the device's file resource list: **Maximum performance**, **Recommended**, and **Maximum protection**.

To select one of the predefined security levels:

1. Open the **Properties: Real-Time File Protection** window.
2. Select the **Protection scope** tab.
3. In the protected device's list, select an item included in the protection scope in order to set a predefined security level.
4. Click the **Configure** button.

   The **Real-time file protection settings** window opens.
5. On the **Security level** tab select the security level to be applied.

   The window displays the list of security settings corresponding to the security level selected.
6. Click the **OK** button.
7. Click the **OK** button in the **Properties: Real-Time File Protection** window.

   Configured task settings are saved and applied immediately to a running task. If the task is not running, the modified settings are applied at next start.

Configuring security settings manually

By default, the Real-Time File Protection task uses common security settings for the entire protection scope. These settings correspond to the **Recommended** predefined security level.

The default values of security settings can be modified by configuring them as common settings for the entire protection scope or as different settings for individual items in the device's file resource list or nodes in the tree.

To configure the security settings of the selected node manually:

1. Open the **Real-time file protection** window.
2. On the **Protection scope** tab, select the node whose security settings you want to configure, and click **Configure**.

   The **Real-time file protection settings** window opens.
3. On the **Security level** tab, click the **Settings** button to customize the configuration.
4. You can configure custom security settings for the selected node in accordance with your requirements:
   - General settings
   - Actions
   - Performance
5. Click the **OK** button in the **Real-time file protection** window.

The new protection scope settings are saved.

Configuring general task settings

To configure the general security settings of the Real-Time File Protection task:

1. Open the **Real-time file protection settings** window.
2. Open the **General** tab.
3. In the **Objects protection** block, specify the object types that you want to include in the protection scope:
   - **All objects**
   - **Objects scanned by format**
   - **Objects scanned according to list of extensions specified in anti-virus database**
   - **Objects scanned by specified list of extensions**
   - **Scan disk boot sectors and MBR**
   - **Scan alternate NTFS streams**
4. In the **Performance** group box, select or clear the **Protect only new and modified files** check box.

   To switch between available options when the check box is cleared, click on the **All** / **Only new** link for each of the compound object types.
5. In the **Compound objects protection** block, specify the compound objects that you want to include in the protection scope:

- **All** / **Only new archives**
- **All** / **Only new SFX archives**
- **All** / **Only new email databases**
- **All** / **Only new packed objects**
- **All** / **Only new plain email**
- **All** / **Only new embedded OLE objects**

6. Click the **Save** button.

The new task configuration will be saved.

Configuring actions

To configure actions on infected and other detected objects during the Real-Time File Protection task:

1. Open the **Real-time file protection settings** window.
2. Select the **Actions** tab.
3. Select the action to be performed on infected and other detected objects:
   - **Notify only**.
   - **Block access**.
   - **Perform additional action**.
     Select the action from the drop-down list:
     - **Disinfect**.
     - **Disinfect. Remove if disinfection fails**.
     - **Remove**.
     - **Recommended**.
4. Select the action to be performed on probably infected objects:
   - **Notify only**.
   - **Block access**.
   - **Perform additional action**
     Select the action from the drop-down list:
     - **Quarantine**.
     - **Remove**.

- **Recommended**.

5. Configure actions to be performed on objects depending on the type of object detected:

   a. Clear or select the **Perform actions depending on the type of object detected** check box.

   b. Click the **Settings** button.

   c. In the window that opens, select a primary action and a secondary action (to be performed if the primary action fails) for each type of detected object.

   d. Click the **OK** button.

6. Select the action to perform on unmodifiable compound files: select or clear the **Entirely remove compound file that cannot be modified by the application in case of embedded object detection** check box.

7. Click the **Save** button.

The new task configuration will be saved.

Configuring performance

To configure performance settings for the Real-Time File Protection task:

1. Open the **Real-time file protection settings** window.

2. Select the **Performance** tab.

3. In the **Exclusions** block:

   - Clear or select the **Exclude files** check box.
   - Clear or select the **Do not detect** check box.
   - Click the **Edit** button for each setting to add exclusions.

4. In the **Advanced settings** block:

   - **Stop scanning if it takes longer than (sec.)**
   - **Do not scan compound objects larger than (MB)**
   - **Use iSwift technology**
   - **Use iChecker technology**

Managing the Real-Time File Protection task via the Application Console

In this section, learn how to navigate the Application Console interface and configure task settings on a protected device.

Navigation

Learn how to navigate to the required task settings via the chosen interface.

Opening the Real-Time File Protection task settings

To open the general task settings window:

1. In the Application Console tree, expand the **Real-Time Computer Protection** node.
2. Select the **Real-Time File Protection** child node.
3. Click the **Properties** link in the results pane.
   The **Task settings** window appears.

Opening the Real-Time File Protection task scope settings

To open the Protection scope settings window for the Real-Time File Protection task:

1. In the Application Console tree, expand the **Real-Time Computer Protection** node.
2. Select the **Real-Time File Protection** child node.
3. Click the **Configure protection scope** link in the results pane.
   The **Protection scope settings** window opens.

Configuring Real-Time File Protection task

To configure the Real-Time File Protection task settings:

1. Open the **Task settings** window.
2. On the **General** tab, configure the following task settings:
   - Objects protection mode
   - **Heuristic analyzer**
   - **Integration with other components**
3. On the **Schedule** and **Advanced** tabs, specify the scheduled start settings.
4. Click the **OK** button in the **Task settings** window.
   The modified settings are saved.

5. In the results pane of the **Real-Time File Protection** node click the **Configure protection scope** link.

6. Do the following:

   - In the tree or list of the device's file resources, select the nodes or items that you want to be included in the task protection scope.

   - Select one of the predefined security levels or configure the object protection settings manually.

7. In the **Protection scope settings** window, click the **Save** button.

   Kaspersky Embedded Systems Security for Windows immediately applies the new settings to the running task. The date and time when the settings were modified and the values of task settings before and after modification are saved in the system audit log.

Selecting protection mode

In the Real-Time File Protection task, the protection mode can be selected. The **Objects protection mode** section lets you specify the type of access attempts for which Kaspersky Embedded Systems Security for Windows scans objects.

The value of the **Objects protection mode** setting applies to the entire protection scope specified in the task. You cannot specify different values for the setting for individual nodes within the protection scope.

To select the protection mode:

1. Open the **Task settings** window.

2. In the window that opens, open the **General** tab and select the protection mode that you want to set:

   - **Smart mode**
   - **On access and modification**
   - **On access**
   - **When run**
   - **Deeper analysis of launching processes (process launch is blocked until the analysis ends)**

3. Click the **OK** button.

   The selected protection mode will take effect.

Configuring Heuristic Analyzer and integration with other application components

To start the KSN Usage task, you must accept the Kaspersky Security Network Statement.

To configure Heuristic Analyzer and integration with other components:

1. Open the **Task settings** window.
2. On the **General** tab, clear or select the **Use heuristic analyzer** check box.
3. If necessary, adjust the level of analysis using the slider.
4. In the **Integration with other components** section, configure the following settings:
   - Select or clear the **Apply Trusted Zone** check box.

     Click the **Trusted Zone** link to open the Trusted Zone settings.
   - Select or clear the **Use KSN for protection** check box.

     The **Send data about scanned files** check box must be selected in the KSN Usage task settings.
   - Select or clear the **Block access to network shared resources for the sessions that show malicious activity** check box.
   - Select or clear the **Launch critical areas scan when active infection is detected** check box.
5. Click the **OK** button.

The newly configured settings are applied.

Configuring the task schedule settings

In the Application Console, you can schedule when to start local system and custom tasks. However, you cannot schedule when to start group tasks.

To schedule a task:

1. Open the context menu of the task you want to schedule.
2. Select **Properties**.

   The **Task settings** window appears.
3. In the window that opens, on the **Schedule** tab, select the **Run by schedule** check box.
4. Follow these steps to specify schedule settings:

   a. In the **Frequency** drop-down menu, select one of the following:

   - **Hourly**: to run the task at some interval measured in hours; specify the number of hours in the **Every <number> hour(s)** field.
   - **Daily**: to run the task at some interval measured in days; specify the number of days in the **Every <number> day(s)** field.
   - **Weekly**: to run the task at some interval measured in weeks; specify the number of weeks in the **Every <number> week(s) on** field. Specify the days of the week on which the task will be started (by default tasks run on Mondays).

- **At application launch**, if you want the task to run every time Kaspersky Embedded Systems Security for Windows starts.
- **After application database update**, if you want the task to run after every update of the application databases.

b. Specify the time for the first task start in the **Start time** field.

c. In the **Start date** field, specify the date when to start the task for the first time.

After you have specified the task start frequency, the time of the first task start, and the date from which the schedule applies, the estimated time for the next task start will appear in the top part of the window in the **Next start** field. The estimated time of the next task start will be updated and displayed each time you open the **Task settings** window on the **Schedule** tab.

The **Next start** field displays the **Blocked by policy** value if Kaspersky Security Center active policy settings prohibit scheduled local system tasks from starting.

5. Use the **Advanced** tab to specify the following schedule settings:

- In the **Task stop settings** section:

  a. Select the **Duration** check box. In the fields to the right, enter maximum task duration in hours and minutes.

  b. Select the **Pause from** check box. In the fields to the right, enter when to pause and resume the task (under 24 hours).

- In the **Advanced settings** block:

  a. Select the **Cancel schedule from** check box and specify the task schedule end date.

  b. Select the **Run skipped tasks** check box to start skipped tasks.

  c. Select the **Randomize the task start within interval of** check box and specify a value in minutes.

6. Click the **OK** button.

The task schedule settings are saved.

Creating the protection scope

This section provides instructions on creating and managing a protection scope in the Real-Time File Protection task.

Configuring the view for network file resources

To select the view for network file resources during configuration of protection scope settings:

1. Open the **Protection scope settings** window.
2. Open the drop-down list in the upper left section of the window and select one of the following options:
   - Select the **Tree-view** option to display the network file resources as a tree.
   - Select the **List-view** option to display the network file resources as a list.

   By default, the network file resources of the protected device are displayed in a list-view mode.
3. Click the **Save** button.

Creating the protection scope

The procedure for creating the Real-Time File Protection task scope depends on the selected network file resource view. You can configure the view of network file resources as a tree or as a list (default view).

To apply the new protection scope settings to the task, the Real-Time File Protection task must be restarted.

To create a protection scope using the network file resource tree:

1. Open the **Protection scope settings** window.
2. In the left section of the window, open the network file resource tree to display all the nodes and child nodes.
3. Do the following:
   - To exclude individual nodes from the protection scope, clear check boxes next to the names of these nodes.
   - To include individual nodes in the protection scope, clear the **My Computer** check box and do the following:
     - If you want to include all drives of the same type in the protection scope, select the check box next to the name of the required type of drives. For example, to include all removable drives on a device, select the **Removable drives** check box.
     - If an individual disk of a certain type is to be included in the protection scope, expand the node that contains the list of drives of this type and check the box next to the name of the required drive. For example, to select the removable drive F:, expand the **Removable drives** node and select the check box for the **F:** drive.
     - If you would like to include only a single folder or file on the drive, select the check box next to the name of that folder or file.
4. Click the **Save** button.

The **Protection scope settings** window closes. The specified settings are saved.

To create a protection scope using the network file resources list:

1. Open the **Protection scope settings** window.

2. To include individual nodes in the protection scope, clear the **My Computer** check box and do the following:

   a. Open the context menu of the protection scope by right-clicking it.

   b. In the context menu of the button, select **Add protection scope**.

   c. In the **Add protection scope** window select an object type to add it to the protection scope:

   - **Predefined scope** - to include one of the predefined scopes in the protection scope on the device. Then in the drop-down list, select the desired protection scope.
   - **Disk, folder or network location** - to include individual drive, folder or a network object in the protection scope. Then select the desired scope by clicking the **Browse** button.
   - **File** - to include an individual file in the protection scope. Then select the desired scope by clicking the **Browse** button.

   You cannot add an object to a protection scope if it has already been added as an exclusion from a protection scope.

3. To exclude individual nodes from the protection scope, clear check boxes next to the names of these nodes or take the following steps:

   a. Open the context menu of the protection scope by right-clicking it.

   b. In the context menu, select the **Add exclusion** option.

   c. In the **Add exclusion** window, select an object type that you want to add as an exclusion from the protection scope following the procedure used when adding an object to the protection scope.

4. To modify the protection scope or an existing exclusion, select the **Edit scope** option in the context menu of the desired protection scope.

5. To hide a previously added protection scope or an exclusion in the list of network file resources, select the **Remove from the list** option in the context menu of the desired protection scope.

   A protection scope is removed from the Real-Time File Protection task scope when it is removed from the network file resource list.

6. Click the **Save** button.

The **Protection scope settings** window closes. The specified settings are saved.

The Real-Time File Protection task can be started if at least one of the device's file resource nodes is included in a protection scope.

If a complex protection scope is specified, for example, if different security values for settings for multiple nodes in the device's file resource tree are specified, this may slow the scanning of objects when they are accessed.

Including network objects in the protection scope

Network drives, folders or files can be added to the protection scope by specifying their path in UNC (Universal Naming Convention) format.

You can scan network folders under the system account.

To add a network location to the protection scope:

1. Open the **Protection scope settings** window.
2. Open the drop-down list in the upper left part of the window and select **Tree-view**.
3. In the context menu of the **Network** node:
   - Select **Add network folder**, if you want to add a network folder to the protection scope.
   - Select **Add network file**, if you want to add a network file to the protection scope.
4. Enter the path to the network folder or file in UNC format.
5. Press the **ENTER** key.
6. Select the check box next to the newly added network object to include it in the protection scope.
7. If necessary, change the security settings for the added network object.
8. Click the **Save** button.

The specified task settings are saved.

Creating a virtual protection scope

You can expand the protection / scan scope by adding individual virtual drives, folders, or files only if the protection / scan scope is presented as a tree of file resources.

To add a virtual drive to the protection scope:

1. Open the **Protection scope settings** window.
2. Open the drop-down list in the upper left part of the window and select **Tree-view**.
3. Open the context menu of the **Virtual drives** node.
4. Select the **Add virtual drive** option.
5. In the list of available names, select the name of the virtual drive that is being created.
6. Select the check box next to the drive to include the drive in the protection scope.

7. In the **Protection scope settings** window, click the **Save** button.

The specified settings are saved.

To add a virtual folder or virtual file to the protection scope:

1. Open the **Protection scope settings** window.
2. Open the drop-down list in the upper left part of the window and select **Tree-view**.
3. Open the context menu of the virtual drive to which you want to add a folder or a file, and select one of the following options:
   - **Add virtual folder** - if you want to add a virtual folder to the protection scope.
   - **Add virtual file** - if you want to add a virtual file to the protection scope.
4. In the entry field, specify the name of the folder or file.
5. In the line containing the name of the created folder or file, select the check box to include the folder or file in the protection scope.
6. In the **Protection scope settings** window, click the **Save** button.

The specified task settings are saved.

Configuring security settings manually

By default Real-Time Computer Protection tasks use common security settings for the entire protection scope. These settings correspond to the **Recommended** predefined security level.

The default values of security settings can be modified by configuring them as common settings for the entire protection scope or as different settings for individual items in the device's file resource list or nodes in the tree.

When working with the protected device's file resource tree, security settings that are configured for the selected parent node are automatically applied to all child nodes. The security settings of the parent node are not applied to child nodes that are configured separately.

To configure security settings manually:

1. Open the **Protection scope settings** window.
2. In the left window section select the node to configure security settings.

   A predefined security settings template can be applied for a selected node or item in the protection scope.

   In the left part of the window, you can select the view for network file resources, create a protection scope, or create a virtual protection scope.
3. In the right part of the window, do one of the following:
   - On the **Security level** tab select the security level to be applied.
   - On the following tabs configure the security settings of the selected node or item in accordance with your requirements:

- General
- Actions
- Performance

4. In the **Protection scope settings** window, click the **Save** button.

The new protection scope settings are saved.

Selecting predefined security levels for Real-Time File Protection task

You can apply one of the following three predefined security levels to a node selected in the protected device's file resource tree or list: **Maximum performance**, **Recommended**, and **Maximum protection**.

To select one of the predefined security levels:

1. Open the **Protection scope settings** window.
2. In the protected device's network file resource tree or list, select a node or item to set the predefined security level.
3. Make sure that the selected node or item is included in the protection scope.
4. In the right part of the window, on the **Security level** tab select the security level to be applied.

   The window displays the list of security settings corresponding to the selected security level.
5. Click the **Save** button.

   The task settings are saved and applied immediately to the running task. If the task is not running, the modified settings are applied at the next start.

Configuring general task settings

To configure the general security settings of the Real-Time File Protection task:

1. Open the **Protection scope settings** window.
2. Open the **General** tab.
3. In the **Objects protection** section, specify the objects that you want to include in the protection scope:
   - All objects
   - Objects scanned by format
   - Objects scanned according to list of extensions specified in anti-virus database
   - Objects scanned by specified list of extensions
   - Scan disk boot sectors and MBR

- Scan alternate NTFS streams

4. In the **Performance** group box, select or clear the Protect only new and modified files check box.

   To switch between available options when the check box is cleared, click on the **All** / **Only new** link for each of the compound object types.

5. In the **Compound objects protection** block, specify the compound objects that you want to include in the protection scope:

   - All / Only new archives
   - All / Only new SFX archives
   - All / Only new email databases
   - All / Only new packed objects
   - All / Only new plain email
   - All / Only new embedded OLE objects

6. Click the **Save** button.

The new task configuration will be saved.

Configuring actions

To configure actions on infected and other detected objects during the Real-Time File Protection task:

1. Open the Protection scope settings window.
2. Select the **Actions** tab.
3. Select the action to be performed on infected and other detected objects:
   - Notify only.
   - Block access.
   - **Perform additional action**.
     Select the action from the drop-down list:
     - **Disinfect**.
     - **Disinfect. Remove if disinfection fails**.
     - Remove.
     - Recommended.
4. Select the action to be performed on probably infected objects:

- Notify only.
- Block access.
- **Perform additional action**

  Select the action from the drop-down list:

  - **Quarantine**.
  - Remove.
  - Recommended.

5. Configure actions to be performed on objects depending on the type of object detected:

   a. Clear or select the Perform actions depending on the type of object detected check box.

   b. Click the **Settings** button.

   c. In the window that opens, select a primary action and a secondary action (to be performed if the primary action fails) for each type of detected object.

   d. Click the **OK** button.

6. Select the action to perform on unmodifiable compound files: select or clear the Entirely remove compound file that cannot be modified by the application in case of embedded object detection check box.

7. Click the **Save** button.

The new task configuration will be saved.

Configuring performance

To configure performance settings for the Real-Time File Protection task:

1. Open the Protection scope settings window.
2. Select the **Performance** tab.
3. In the **Exclusions** block:
   - Clear or select the Exclude files check box.
   - Clear or select the Do not detect check box.
   - Click the **Edit** button for each setting to add exclusions.
4. In the **Advanced settings** block:
   - Stop scanning if it takes longer than (sec.)
   - Do not scan compound objects larger than (MB)
   - Use iSwift technology

- Use iChecker technology

Real-Time File Protection task statistics

When the Real-Time File Protection task is running, you can view detailed real-time information about the number of objects processed by Kaspersky Embedded Systems Security for Windows since the task was started.

To view the Real-Time File Protection task statistics:

1. In the Application Console tree, expand the **Real-Time Computer Protection** node.
2. Select the **Real-Time File Protection** child node.

   Task statistics are displayed in the **Statistics** section of the results pane of the selected node.

The information can be viewed about objects processed by Kaspersky Embedded Systems Security for Windows since it was started (see the table below).

Real-Time File Protection task statistics

Field	Description
Detected	Number of objects detected by Kaspersky Embedded Systems Security for Windows. For example, if Kaspersky Embedded Systems Security for Windows detects one malicious object in five files, the value in this field increases by one.
Infected and other objects detected	Number of objects that Kaspersky Embedded Systems Security for Windows found and classified as infected, or number of found legitimate software files that can be used by intruders to damage your device or personal data.
Probably infected objects detected	Number of objects found by Kaspersky Embedded Systems Security for Windows to be probably infected.
Objects not disinfected	Number of objects that Kaspersky Embedded Systems Security for Windows did not disinfect for the following reasons: • The detected object is of a type that cannot be disinfected. • An error occurred during disinfection.
Objects not moved to Quarantine	Number of objects that Kaspersky Embedded Systems Security for Windows attempted to quarantine unsuccessfully, for example, due to insufficient disk space.
Objects not removed	Number of objects that Kaspersky Embedded Systems Security for Windows attempted to delete unsuccessfully, because, for example, access to the object was blocked by another application.
Objects not scanned	Number of objects in the protection scope that Kaspersky Embedded Systems Security for Windows failed to scan, because, for example, access to the object was blocked by another application.
Objects not backed up	Number of objects whose copies Kaspersky Embedded Systems Security for Windows attempted to save in Backup unsuccessfully, for example, due to insufficient disk space.
Processing	Number of objects whose processing resulted in an error.

errors	
Objects disinfected	Number of objects disinfected by Kaspersky Embedded Systems Security for Windows.
Moved to Quarantine	Number of objects quarantined by Kaspersky Embedded Systems Security for Windows.
Moved to Backup	Number of objects whose copies Kaspersky Embedded Systems Security for Windows saved to Backup.
Objects removed	Number of objects removed by Kaspersky Embedded Systems Security for Windows.
Password-protected objects	Number of objects (archives, for example) that Kaspersky Embedded Systems Security for Windows skipped because they were password protected.
Corrupted objects	Number of objects skipped by Kaspersky Embedded Systems Security for Windows because their format was corrupted.
Objects processed	Total number of objects processed by Kaspersky Embedded Systems Security for Windows.

You can view the Real-Time File Protection task statistics in the task log by clicking the **Open task log** link in the **Management** section of the detail pane.

If the value of the **Total events** field in the Real-Time File Protection task log window exceeds 0, we recommend that you manually process the events in the task log on the **Events** tab.

Managing Real-Time File Protection task via the Web Plug-in

In this section, learn how to manage the Real-Time File Protection task via the Web Plug-in interface.

Configuring Real-Time File Protection task

Predefined security level can not be changed for the Real-Time File Protection task via the Web Plug-in.

To configure the Real-Time File Protection task via the Web Plug-in:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.
2. Click the policy name you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.
4. Select the **Real-time computer protection** section.
5. Click **Settings** in the **Real-Time File Protection** subsection.
6. Configure the settings described in the table below.

Setting	Description
Smart mode	Kaspersky Embedded Systems Security for Windows selects objects to be scanned on its own. An object is scanned on being opened and then again after being saved if the object has been modified. If the object is accessed multiple times and modified by the process, Kaspersky Embedded Systems Security for Windows rescans the object only after the object is saved by the process for the last time.
On access	Kaspersky Embedded Systems Security for Windows scans all objects when they are opened for reading, execution, or modification.
On access and modification	Kaspersky Embedded Systems Security for Windows scans an object when it is opened and rescans after it is saved, if the object was modified. This option is selected by default.
When run	Kaspersky Embedded Systems Security for Windows scans a file only when it is accessed to be executed.
Deeper analysis of launching processes (process launch is blocked until the analysis ends)	Kaspersky Embedded Systems Security for Windows performs longer analysis of launching processes with higher probability to detect a threat. The process launch is blocked until the end of analysis.
Use Heuristic Analyzer	This check box enables / disables Heuristic Analyzer during object scanning. If the check box is selected, Heuristic Analyzer is enabled. If the check box is cleared, Heuristic Analyzer is disabled. The check box is selected by default.
Heuristic analysis level	The heuristic analysis level sets the balance between the thoroughness of searches for threats, the load on the operating system's resources and the time required for scanning. The following scanning sensitivity levels are available: • **Light**. Heuristic Analyzer performs fewer instructions within executable files. The probability of threat detection in this mode is somewhat lower. Scanning is faster and less resource-intensive. • **Medium**. Heuristic Analyzer performs the number of executable file instructions recommended by Kaspersky experts. This level is selected by default. • **Deep**. Heuristic Analyzer performs more instructions within executable files. The probability of threat detection in this mode is higher. Scanning uses more system resources, takes more time, and can produce a higher number of false alarms. The setting is available if the **Use heuristic analyzer** check box is selected.
Apply Trusted Zone	This check box enables / disables use of the Trusted Zone for a task. If the check box is selected, Kaspersky Embedded Systems Security for Windows adds file operations of trusted processes to the scan exclusions configured in the task settings.

	If the check box is cleared, Kaspersky Embedded Systems Security for Windows disregards the file operations of trusted processes when forming the protection scope for the task. The check box is selected by default.
Use KSN for protection	This check box enables or disables the use of KSN services. If the check box is selected, the application uses Kaspersky Security Network data to ensure that the application responds more quickly to new threats and to reduce the likelihood of false positives. If the check box is cleared, the task does not use KSN services. The check box is selected by default.
Block access to network shared resources for the network sessions showing malicious activity	The check box enables or disables blocking current session and controls the availability of network shared resources in terms of current session. If the check box is selected, Kaspersky Embedded Systems Security for Windows blocks current session and, in terms of current session, makes network shared resources unavailable for hosts for which malicious activity was detected in the Blocked hosts storage section If the check box is cleared, conditions are not applied and Kaspersky Embedded Systems Security for Windows functions typically. By default, the check box is cleared. You can view the list of blocked hosts in the Blocked Hosts storage. You can restore access to blocked hosts, and specify the number of days, hours, and minutes after which hosts regain access to network file resources after being blocked by configuring the Blocked Hosts storage settings.
Launch critical areas scan when active infection is detected	If the check box is selected, when active infection is detected, Kaspersky Embedded Systems Security for Windows creates and launches a temporary Critical Areas Scan task. When the Critical Areas Scan temporary task finishes, Kaspersky Embedded Systems Security for Windows removes this temporary task. If the check box is cleared, when active infection is detected, Kaspersky Embedded Systems Security for Windows does not create and launch Critical Areas Scan task. The check box is selected by default.
Protection scope	You can configure security settings of the protection scope.

Configuring the task protection scope

To configure a protection scope for Real-Time File Protection task:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.
2. Click the policy name you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.
4. Select the **Real-time computer protection** section.

5. Click **Settings** in the **Real-Time File Protection** subsection.
6. Select the **Protection scope** section.
7. Do one of the following:
   - Click the **Add** button to add a new rule.
   - Select an existing rule and click **Edit** button.

   The **Edit scope** window opens.
8. Switch the toggle button to **Active** and select an object type.
9. In the **Objects protection** section, configure the following settings:
   - **Objects protection mode**:
     - All objects
     - Objects scanned by format
     - Objects scanned according to list of extensions specified in anti-virus database
     - Objects scanned by specified list of extensions
   - Scan disk boot sectors and MBR
   - Scan alternate NTFS streams
10. In the **Objects protection** section, select or clear the Protect only new and modified files check box.
11. In the **Compound objects protection** section, specify the compound objects that you want to include in the scan scope:
    - Archives
    - SFX archives
    - Packed objects
    - Email databases
    - Plain email
    - Embedded OLE objects
    - Entirely remove compound file that cannot be modified by the application in case of embedded object detection
12. Select the action to be performed on infected and other detected objects:
    - Notify only
    - Block access

- **Perform additional action**.

  Select the action from the drop-down list:

  - **Disinfect**.
  - **Disinfect. Remove if disinfection fails**.
  - **Remove**.
  - **Recommended**.

13. Select the action to be performed on probably infected objects:

- **Notify only**.
- **Block access**.
- **Perform additional action**.

  Select the action from the drop-down list:

  - **Quarantine**.
  - **Remove**.
  - **Recommended**.

14. Configure actions to be performed on objects depending on the type of object detected:

    a. Clear or select the **Perform actions depending on the type of object detected** check box.

    b. Click the **Settings** button.

    c. In the window that opens, select a primary action and a secondary action (to be performed if the primary action fails) for each type of detected object.

    d. Click the **OK** button.

15. In the **Exclusions** section, configure the following settings:

- Clear or select the **Exclude files** check box.
- Clear or select the **Do not detect** check box.

16. In the **Performance** section, configure the following settings:

- **Stop scanning if it takes longer than (sec)**
- **Do not scan compound objects larger than (MB)**
- **Use iSwift technology**
- **Use iChecker technology**

17. Click the **OK** button.

KSN Usage

This section contains information about the KSN Usage task and how to configure it.

Updates functionality (including providing anti-virus signature updates and codebase updates), as well as KSN functionality may not be available in the program in the U.S.

About the KSN Usage task

Kaspersky Security Network (also referred to as "KSN") is an infrastructure of online services providing access to Kaspersky's operative knowledge base on the reputation of files, web resources and programs. Kaspersky Security Network allows Kaspersky Embedded Systems Security for Windows to react very promptly to new threats, improves the performance of several protection components, and reduces the likelihood of false positives.

To start the KSN Usage task, you must accept the Kaspersky Security Network Statement.

Information received by Kaspersky Embedded Systems Security for Windows from Kaspersky Security Network pertains only to the reputation of programs.

Participation in KSN allows Kaspersky to receive real-time information about types and sources of new threats, develop ways to neutralize them, and reduce the number of false positives in application components.

More detailed information about the transferring, processing, storage, and destruction of information about application usage is available in the **Kaspersky Security Network Statement** window of the KSN Usage task, and in the Privacy Policy on the Kaspersky's website.

Participation in Kaspersky Security Network is voluntary. The decision regarding participation in Kaspersky Security Network is made after installation of Kaspersky Embedded Systems Security for Windows. You can change your decision about participation in Kaspersky Security Network at any time.

Kaspersky Security Network can be used in the following Kaspersky Embedded Systems Security for Windows tasks:

- Real-Time File Protection.
- On-Demand Scan.
- Applications Launch Control rules

Kaspersky Private Security Network

See details about how to configure Kaspersky Private Security Network (hereinafter referred to "Private KSN") in the *Kaspersky Security Center Help*.

If you use Private KSN on the device, in the **Kaspersky Security Network Statement** window of the KSN Usage task you can read the KSN Statement and enable the task by selecting the **I accept the terms of participation in Kaspersky Security Network** check box. By accepting the terms you agree to send all types of data mentioned in KSN Statement (security requests, statistical data) to KSN services.

After accepting the Private KSN terms, the check boxes that adjust the Global KSN usage are not available.

If you disable Private KSN when the KSN Usage task is running, the *License violation* error occurs and the task stops. To continue protecting the device you need to accept the KSN Statement in the **Kaspersky Security Network Statement** window and restart the task.

Withdrawal of the KSN Statement acceptance

You can withdraw the acceptance and stop any data exchange with the Kaspersky Security Network at any moment. The following actions are considered as the full or partial withdrawal of KSN Statement:

- Clearing the **Send data about scanned files** check box: the application stops sending checksums of scanned files to KSN service for analysis.
- Clearing the **Send Kaspersky Security Network statistics** check box: the application stops processing data with additional KSN statistics.
- Clearing the **I accept the terms of participation in Kaspersky Security Network** check box: the application stops all KSN-related data processing, the KSN Usage task stops.
- Uninstalling the KSN Usage component: all KSN-related data processing stops.
- Uninstalling the Kaspersky Embedded Systems Security for Windows: all KSN-related data processing stops.
- Uninstalling a license key for the Kaspersky Embedded Systems Security for Windows or the license is suspended: all KSN-related data processing stops.

Default KSN Usage task settings

You can change the default settings of the KSN Usage task (see the table below).

Default KSN Usage task settings

Setting	Default value	Description
Action to perform on KSN untrusted objects	Remove	You can specify actions that Kaspersky Embedded Systems Security for Windows will take on objects identified by KSN as untrusted.
Data transfer	The file checksum (MD5 hash) is calculated for files that do not exceed 2 MB in size.	You can specify the maximum size of files for which a checksum is calculated using the MD5 algorithm for delivery to KSN. If the check box is cleared, Kaspersky Embedded Systems Security for Windows calculates the MD5 hash for files of any size.
Task start schedule	First run is not scheduled.	You can start the task manually or configure a scheduled start.

Use Kaspersky Security Center as KSN Proxy	Selected	By default the data is sent to KSN via Kaspersky Security Center. You can change this setting only via the Administration Plug-in.
I accept the terms of participation in Kaspersky Security Network	Cleared	If selected, participation in KSN after the installation is accepted. You can change your decision at any moment.
Send Kaspersky Security Network statistics	Selected (applied only if the KSN Statement is accepted)	If the KSN Statement is accepted, the KSN Statistics will be sent automatically, unless you clear the check box.
Send data about scanned files	Selected (applied only if the KSN Statement is accepted)	If the KSN Statement is accepted, the data about files that were scanned and analyzed since the task has been started, is sent. You can clear the check box at any time.

Managing KSN Usage via the Administration Plug-In

In this section, learn how configure the KSN Usage task and Data Handling via the Administration Plug-In.

Configuring KSN Usage task

To configure the KSN Usage task:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of protected devices, select the **Policies** tab and open the **Properties: <Policy name>** window.
   - To configure the settings of a task or application for an individual protected device, select the **Devices** tab and go to local task settings or application settings.
4. In the **Real-Time Computer Protection** section, click the **Settings** button in the **KSN Usage** subsection.

   The **KSN Usage** window opens.
5. On the **General** tab, configure the following task settings:
   - In the **Action to perform on KSN untrusted objects** section, specify the action that Kaspersky Embedded Systems Security for Windows is to perform if it detects an object identified by KSN as untrusted:
     - Remove

- Log information

- In the **Data transfer** section, restrict the size of files for which the checksum is calculated:
  - Clear or select the **Do not calculate checksum before sending to KSN if file size exceeds (MB)** check box.
  - If required, in the field to the right, change the maximum size of files for which Kaspersky Embedded Systems Security for Windows calculates the checksum.
- In the **KSN Proxy** section, clear or select the **Use Kaspersky Security Center as KSN Proxy** check box.

  To enable KSN Proxy the KSN Statement must be accepted and Kaspersky Security Center properly configured. See *Kaspersky Security Center Help* for more details.

6. If necessary, configure the task start schedule settings on the **Task management** tab. For example, you can enable task start by schedule and specify the start frequency of the **At application launch** if you want the task to run automatically when the protected device is restarted.

   The application will automatically start the KSN Usage task by schedule.

7. Configure the data handling before starting the task.

8. Click the **OK** button.

The modified settings are applied. The date and time of modifying the settings, as well as information about the task settings before and after modification, are saved in the system audit log.

Configuring Data Processing

To configure what data will be processed by the KSN services and accept the KSN Statement:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.

2. Select the administration group for which you want to configure application settings.

3. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of protected devices, select the **Policies** tab and open the **Properties: <Policy name>** window.
   - To configure the settings of a task or application for an individual protected device, select the **Devices** tab and go to local task settings or application settings.

4. In the **Real-Time Computer Protection** section click the **KSN Statement** button in the **KSN Usage** subsection.

   The **Kaspersky Security Network Statement** window opens.

5. On the **Statistics and services** tab, read the Statement and select the **I accept the terms of participation in Kaspersky Security Network** check box.

   KSN Usage will be enabled.

If KSN Usage is enabled in the policy (**I accept the terms of participation in Kaspersky Security Network** check box is selected) and the version of the KSN Statement in the policy differs from the version of the KSN Statement in Kaspersky Embedded Systems Security for Windows installed on the host, then after applying the policy, KSN Usage is disabled on the host and in the policy settings (**I accept the terms of participation in Kaspersky Security Network** check box is cleared). This situation may arise if Kaspersky Embedded Systems Security for Windows 3.4 for Windows is installed on the host, and the version of the Kaspersky Embedded Systems Security for Windows Administration Plug-in with which the policy was last modified is below.

6. To increase the protection level, the following check boxes are automatically selected:

   - **Send data about scanned files**
   - **Send Kaspersky Security Network statistics**

   You can clear these check boxes and stop sending additional data at any moment.

7. The **Send Kaspersky Security Network statistics** check box is selected by default. You can clear the check box at any time if you don't want Kaspersky Embedded Systems Security for Windows to send additional statistics to Kaspersky.

8. Click the **OK** button.

   The data processing configuration will be saved.

Managing KSN Usage via the Application Console

In this section, learn how configure the KSN Usage task and Data handling via the Application Console.

Configuring KSN Usage task

To configure the KSN Usage task:

1. In the Application Console tree, expand the **Real-Time Computer Protection** node.

2. Select the **KSN Usage** child node.

3. Click the **Properties** link in the results pane.

   The **Task settings** window opens on the **General** tab.

4. Configure the task:

   - In the **Action to perform on KSN untrusted objects** section, specify the action that Kaspersky Embedded Systems Security for Windows is to perform if it detects an object identified by KSN as untrusted:

     - **Remove**
     - **Log information**

   - In the **Data transfer** section, restrict the size of files for which the checksum is calculated:

- Clear or select the **Do not calculate checksum before sending to KSN if file size exceeds (MB)** check box.
- If required, in the field to the right, change the maximum size of files for which Kaspersky Embedded Systems Security for Windows calculates the checksum.

5. If needed, configure the task start schedule on the **Schedule** and **Advanced** tabs. For example, you can enable task start by schedule and specify the start frequency of the **At application launch** if you want the task to run automatically when the protected device is restarted.

   The application will automatically start the KSN Usage task by schedule.

6. Configure the data handling before starting the task.

7. Click the **OK** button.

The modified settings are applied. The date and time of modifying the settings, as well as information about the task settings before and after modification, are saved in the system audit log.

Configuring Data Processing

To configure what data will be processed by the KSN services and accept the KSN Statement:

1. In the Application Console tree, expand the **Real-Time Computer Protection** node.

2. Select the **KSN Usage** child node.

3. Click the **KSN Statement** link in the details pane.

   The **Kaspersky Security Network Statement** window opens.

4. On the **Statistics and services** tab, read the Statement and select the **I accept the terms of participation in Kaspersky Security Network** check box.

   KSN Usage will be enabled.

   If KSN Usage is enabled in the policy (**I accept the terms of participation in Kaspersky Security Network** check box is selected) and the version of the KSN Statement in the policy differs from the version of the KSN Statement in Kaspersky Embedded Systems Security for Windows installed on the host, then after applying the policy, KSN Usage is disabled on the host and in the policy settings (**I accept the terms of participation in Kaspersky Security Network** check box is cleared). This situation may arise if Kaspersky Embedded Systems Security for Windows 3.4 for Windows is installed on the host, and the version of the Kaspersky Embedded Systems Security for Windows Administration Plug-in with which the policy was last modified is below.

5. To increase the protection level, the following check boxes are automatically selected:

   - **Send data about scanned files**
   - **Send Kaspersky Security Network statistics**

   You can clear these check boxes and stop sending additional data at any moment.

6. The **Send Kaspersky Security Network statistics** check box is selected by default. You can clear the check box at any time if you don't want Kaspersky Embedded Systems Security for Windows to send additional statistics to Kaspersky.

7. Click the **OK** button.

The data processing configuration will be saved.

Managing KSN Usage via the Web Plug-in

To configure the KSN Usage task and Data Handling via the Web Plug-in:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.

2. Click the policy name you want to configure.

3. In the **<Policy name>** window that opens, select the **Application settings** tab.

4. Select the **Real-time computer protection** section.

5. Click **Settings** in the **KSN Usage** subsection.

6. Configure the settings described in the table below.

KSN Usage task and Data Handling via the Administration Plug-In settings

Setting	Description
Remove	Kaspersky Embedded Systems Security for Windows deletes the object with KSN-untrusted status and places a copy of it in Backup. This option is selected by default.
Log information	Kaspersky Embedded Systems Security for Windows records information about the object with KSN-untrusted status in the task log. Kaspersky Embedded Systems Security for Windows does not delete the untrusted object.
Do not calculate checksum before sending to KSN if file size exceeds	This check box enables or disables calculation of the checksum for files of the specified size for delivery of this information to the KSN service. The duration of the checksum calculation depends on the file size. If this check box is selected, Kaspersky Embedded Systems Security for Windows does not calculate the checksum for files that exceed the specified size (in MB). If the check box is cleared, Kaspersky Embedded Systems Security for Windows calculates the checksum for files of any size. The check box is selected by default.
I confirm that I have fully read, understood, and accept the terms of participation in Kaspersky	By selecting this check box you confirm that you have read and accepted the terms of the Kaspersky Security Network Statement.

Security Network	If KSN Usage is enabled in the policy (**I accept the terms of participation in Kaspersky Security Network** check box is selected) and the version of the KSN Statement in the policy differs from the version of the KSN Statement in Kaspersky Embedded Systems Security for Windows installed on the host, then after applying the policy, KSN Usage is disabled on the host and in the policy settings (**I accept the terms of participation in Kaspersky Security Network** check box is cleared). This situation may arise if Kaspersky Embedded Systems Security for Windows 3.4 for Windows is installed on the host, and the version of the Kaspersky Embedded Systems Security for Windows Administration Plug-in with which the policy was last modified is below.
Send data about scanned files	If the check box is selected, Kaspersky Embedded Systems Security for Windows sends the checksum of scanned files to the Kaspersky. Conclusion about each file security is based on the reputation received from KSN. If the check box is cleared, Kaspersky Embedded Systems Security for Windows does not send checksum of files to KSN. Note, than the file reputation requests might be sent in a limited mode. The limitations are used for protection of the Kaspersky reputation servers from the DDoS attacks. In this scenario, the parameters of file reputation requests, that are being sent, are defined by the rules and methods established by the Kaspersky experts and cannot be configured by user on a protected device. Updates of these rules and methods are received along with the application database updates. If the limitations are applied, the *enabled by Kaspersky for protecting KSN servers against DDoS* status is displayed in the KSN Usage task statistics. The check box is selected by default.
Agree to process data as a part of the Kaspersky Security Network statistics	If the check box is selected the Kaspersky Embedded Systems Security for Windows sends additional statistics, which may contain personal data. The list of all data, that is sent as KSN statistics, is specified in the KSN Statement. The data received by Kaspersky is used to improve the quality of applications and level of threat detection rates. If the check box is cleared, Kaspersky Embedded Systems Security for Windows does not send additional statistics. The check box is selected by default.
Task management	You can configure settings to start the task on a schedule.

Configuring additional data transfer

Kaspersky Embedded Systems Security for Windows can be configured to send the following data to Kaspersky:

- Checksums of scanned files (**Send data about scanned files** check box).
- Additional statistics, including personal data (**Send Kaspersky Security Network statistics** check box).

See the "Local data handling" section of this guide for detailed information about data that is sent to Kaspersky.

The corresponding check boxes can be selected or cleared only if the **I accept the terms of participation in Kaspersky Security Network** check box is selected.

By default Kaspersky Embedded Systems Security for Windows sends checksums of files and additional statistics after you accept the KSN Statement.

The **I accept the terms of participation in Kaspersky Security Network** check box is not editable only if the Kaspersky Security Center policy blocks changes of the data handling settings.

Possible check box states and corresponding conditions

Check box state	Conditions for the Send data about scanned files check box state	Conditions for the Send Kaspersky Security Network statistics check box state	Conditions for the I accept the terms of participation in Kaspersky Security Network check box state
☑	• reputation requests are sent • check box is editable	• additional statistics is sent • check box is editable	• the terms of the Kaspersky Security Network Statement are accepted • check box is editable
☑	• reputation requests are sent • check box is not editable	• additional statistics is sent • check box is not editable	• the terms of the Kaspersky Security Network Statement are accepted • check box is not editable
☐	• reputation requests are not sent • check box is editable	• additional statistics is not sent • check box is editable	• the terms of the Kaspersky Security Network Statement are not accepted • check box is editable
☐	• reputation requests are not sent • check box is not editable	• additional statistics is not sent • check box is not editable	• the terms of the Kaspersky Security Network Statement are not accepted • check box is not editable

KSN Usage task statistics

While the KSN Usage task is being executed, detailed information can be viewed in real time about the number of objects processed by Kaspersky Embedded Systems Security for Windows since it was started up till now. Information about all events that occur during the task performing is recorded in the task log.

To view KSN Usage task statistics:

1. In the Application Console tree, expand the **Real-Time Computer Protection** node.
2. Select the **KSN Usage** child node.

Task statistics are displayed in the **Statistics** section of the details pane of the selected node.

You can view information about objects processed by Kaspersky Embedded Systems Security for Windows since the task was started (see the table below).

KSN Usage task statistics

Field	Description
Request sending errors	Number of KSN requests whose processing resulted in a task error.
Statistics formed	Number of generated statistic packages sent to KSN.
Objects removed	Number of objects that Kaspersky Embedded Systems Security for Windows deleted when running the KSN Usage task.
Moved to Backup	Number of objects whose copies Kaspersky Embedded Systems Security for Windows saved to Backup.
Objects not removed	The number of objects that Kaspersky Embedded Systems Security for Windows attempted but was unable to delete, because, for example, access to the object was blocked by another application. Information about such objects is recorded in the task log.
Objects not backed up	The number of objects the copies of which Kaspersky Embedded Systems Security for Windows attempted to save in Backup but was unable to do so, for example, due to insufficient disk space. The application does not disinfect or delete files that it could not move to Backup. Information about such objects is recorded in the task log.
Limited mode	The status signifies whether the application sends file reputation requests in a limited mode. In a limited mode Kaspersky Embedded Systems Security for Windows sends only a part of file reputation requests according to Kaspersky experts recommendation.

Network Threat Protection

This section contains information about the Network Threat Protection task and how to configure it.

About the Network Threat Protection task

The Network Threat Protection can only be installed on a device running Microsoft Windows 7 and any later version or Windows Server 2008 R2 and any later version.

The Network Threat Protection task scans inbound network traffic for activity that is typical of network attacks. Upon detecting an attempted network attack that targets your computer, Kaspersky Embedded Systems Security for Windows blocks network activity from the attacking computer. Your screen then displays a warning stating that a network attack was attempted, and shows information about the attacking computer.

By default, the Network Threat Protection task runs in the **Block connections when attack is detected** mode. In this mode, Kaspersky Embedded Systems Security for Windows adds IP addresses of hosts showing activity typical of network attacks to the list of blocked hosts.

You can view the list of blocked hosts in the Blocked Hosts storage.

You can restore access to blocked hosts, and specify the number of days, hours, and minutes after which hosts regain access to network file resources after being blocked by configuring the Blocked Hosts storage settings.

The IP addresses of hosts showing activity typical of network attacks are deleted from the list of blocked hosts in the following cases:

- Kaspersky Embedded Systems Security for Windows is uninstalled.
- The IP address was deleted manually from the list of blocked hosts.
- Host blocking term has expired.
- The Network Threat Protection task was stopped and the **Don't stop traffic analysis when the task is not running** check boxed is cleared.
- The **Block connections when attack is detected** mode was turned off.

Default Network Threat Protection task settings

The Network Threat Protection task uses the default settings described in the table below. You can change the values of these settings.

Default Network Threat Protection task settings

Setting	Default value	Description
Operating mode	**Block connections when attack is detected**	The Network Threat Protection task can be started in **Pass-through**, **Only inform about network attacks** or **Block connections when attack is detected** mode.

		The check box enables or disables adding hosts showing activity typical of network attacks to the list of blocked hosts. If this mode is selected, Kaspersky Embedded Systems Security for Windows scans inbound network traffic for activity that is typical of network attacks, logs events about detected activity, and adds IP addresses of hosts showing activity typical of network attacks to the list of blocked hosts. You can view the list of blocked hosts in the Blocked Hosts storage. You can restore access to blocked hosts, and specify the number of days, hours, and minutes after which hosts regain access to network file resources after being blocked by configuring the Blocked Hosts storage settings. The mode is selected by default. If this mode is selected, Kaspersky Embedded Systems Security for Windows scans inbound network traffic for activity that is typical of network attacks, logs events about detected activity, but doesn't block network activity from the attacking computer. If this mode is selected, Kaspersky Embedded Systems Security for Windows scans inbound network traffic for activity that is typical of network attacks, but doesn't log events about detected activity and doesn't block network activity from the attacking computer. For example, you can use this mode in case of a decrease in the protected device's performance.
Exclusions	The exclusion list is not applied.	Specify areas that you want to exclude from the task protection scope.
Schedule settings	By default, the Network Threat Protection task starts automatically when Kaspersky Embedded Systems Security for Windows starts.	You can configure the schedule.

Configuring the Network Threat Protection task via the Application Console

In this section, learn how to manage the Network Threat Protection task via the Application Console interface.

General task settings

To configure the general settings of the Network Threat Protection task via the Application Console:

1. In the Application Console tree, expand the **Real-Time Computer Protection** node.
2. Select the **Network Threat Protection** child node.
3. Click the **Network Threat Protection** link in the details pane of the **Properties** node.

   The **Task settings** window appears.
4. Open the **General** tab.
5. In the **Operating mode** section, select the task mode:

   - **Pass-through**.

     If this mode is selected, Kaspersky Embedded Systems Security for Windows scans inbound network traffic for activity that is typical of network attacks, but doesn't log events about detected activity and doesn't block network activity from the attacking computer.

     For example, you can use this mode in case of a decrease in the protected device's performance.

   - **Only inform about network attacks**.

     If this mode is selected, Kaspersky Embedded Systems Security for Windows scans inbound network traffic for activity that is typical of network attacks, logs events about detected activity, but doesn't block network activity from the attacking computer.

   - **Block connections when attack is detected**.

     The check box enables or disables adding hosts showing activity typical of network attacks to the list of blocked hosts.

     If this mode is selected, Kaspersky Embedded Systems Security for Windows scans inbound network traffic for activity that is typical of network attacks, logs events about detected activity, and adds IP addresses of hosts showing activity typical of network attacks to the list of blocked hosts.

     You can view the list of blocked hosts in the Blocked Hosts storage.

     You can restore access to blocked hosts, and specify the number of days, hours, and minutes after which hosts regain access to network file resources after being blocked by configuring the Blocked Hosts storage settings.

     The mode is selected by default.
6. In the **MAC spoofing protection** block, select or clear the **Enable protection against MAC spoofing attacks** check box.

A MAC address spoofing attack consists of changing the MAC address of a network device (network card). As a result, an attacker could redirect data sent to a device to another device and gain access to this data.

If the check box is selected and the Network Threat Protection task mode is different from **Pass-through**, Kaspersky Embedded Systems Security for Windows scans incoming network traffic for actions that are typical of MAC address spoofing attacks and performs actions in accordance with the selected task mode for the Network Threat Protection task.

If the check box is cleared or the **Pass-through** task mode is selected, Kaspersky Embedded Systems Security for Windows does not scan incoming network traffic for actions typical of MAC address spoofing attacks.

By default, the check box is cleared.

7. Select or clear the **Don't stop traffic analysis when the task is not running** check box.

   If this check box is selected, then even when the Network Threat Protection task is stopped, Kaspersky Embedded Systems Security for Windows scans inbound network traffic for activity that is typical of network attacks and blocks network activity from the attacking computer, depending on the selected task mode.

   If this check box is cleared, when the Network Threat Protection task is stopped, Kaspersky Embedded Systems Security for Windows doesn't scan inbound network traffic for activity that is typical of network attacks.

   By default, the check box is cleared.

8. Click the **OK** button.

Adding exclusions

To add exclusions for Network Threat Protection task, take the following steps:

1. In the Application Console tree, expand the **Real-Time Computer Protection** node.
2. Select the **Network Threat Protection** child node.
3. Click the **Network Threat Protection** link in the details pane of the **Properties** node.

   The **Task settings** window appears.

4. On the **Exclusions** tab, select the **Do not control excluded IP-addresses** check box.

   If this check box is selected, Kaspersky Embedded Systems Security for Windows doesn't scan inbound network traffic for excluded IP addresses.

   If this check box is cleared, Kaspersky Embedded Systems Security for Windows doesn't apply the exclusion list.

5. Specify the IP address and click **Add** button.
6. Click the **OK** button.

Configuring the Network Threat Protection task via the Administration Plug-in

In this section, learn how to manage the Network Threat Protection task via the Administration Plug-in interface.

General task settings

To configure the Network Threat Protection task via the Administration Plug-in:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of protected devices, select the **Policies** tab and open the **Properties: <Policy name>** window.
   - To configure the settings of a task or application for an individual protected device, select the **Devices** tab and go to local task settings or application settings.
4. In the **Real-Time Computer Protection** section, in the **Network Threat Protection** block, click the **Settings** button.

   The **Network Threat Protection** window opens.
5. Open the **General** tab.
6. Select the task mode in the **Operating mode** section:
   - **Pass-through**.

     If this mode is selected, Kaspersky Embedded Systems Security for Windows scans inbound network traffic for activity that is typical of network attacks, but doesn't log events about detected activity and doesn't block network activity from the attacking computer.

     For example, you can use this mode in case of a decrease in the protected device's performance.
   - **Only inform about network attacks**.

     If this mode is selected, Kaspersky Embedded Systems Security for Windows scans inbound network traffic for activity that is typical of network attacks, logs events about detected activity, but doesn't block network activity from the attacking computer.
   - **Block connections when attack is detected**.

The check box enables or disables adding hosts showing activity typical of network attacks to the list of blocked hosts.

If this mode is selected, Kaspersky Embedded Systems Security for Windows scans inbound network traffic for activity that is typical of network attacks, logs events about detected activity, and adds IP addresses of hosts showing activity typical of network attacks to the list of blocked hosts.

You can view the list of blocked hosts in the Blocked Hosts storage.

You can restore access to blocked hosts, and specify the number of days, hours, and minutes after which hosts regain access to network file resources after being blocked by configuring the Blocked Hosts storage settings.

The mode is selected by default.

7. In the **MAC spoofing protection** block, select or clear the **Enable protection against MAC spoofing attacks** check box.

   A MAC address spoofing attack consists of changing the MAC address of a network device (network card). As a result, an attacker could redirect data sent to a device to another device and gain access to this data.

   If the check box is selected and the Network Threat Protection task mode is different from **Pass-through**, Kaspersky Embedded Systems Security for Windows scans incoming network traffic for actions that are typical of MAC address spoofing attacks and performs actions in accordance with the selected task mode for the Network Threat Protection task.

   If the check box is cleared or the **Pass-through** task mode is selected, Kaspersky Embedded Systems Security for Windows does not scan incoming network traffic for actions typical of MAC address spoofing attacks.

   By default, the check box is cleared.

8. Select or clear the **Don't stop traffic analysis when the task is not running** check box.

   If this check box is selected, then even when the Network Threat Protection task is stopped, Kaspersky Embedded Systems Security for Windows scans inbound network traffic for activity that is typical of network attacks and blocks network activity from the attacking computer, depending on the selected task mode.

   If this check box is cleared, when the Network Threat Protection task is stopped, Kaspersky Embedded Systems Security for Windows doesn't scan inbound network traffic for activity that is typical of network attacks.

   By default, the check box is cleared.

9. Click the **OK** button.

Adding exclusions

To add exclusions for Network Threat Protection task, take the following steps:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:

- To configure application settings for a group of protected devices, select the **Policies** tab and open the **Properties: <Policy name>** window.
- To configure the settings of a task or application for an individual protected device, select the **Devices** tab and go to local task settings or application settings.

4. In the **Real-Time Computer Protection** section, click the **Settings** button in the **Network Threat Protection** subsection.

   The **Network Threat Protection** window opens.

5. On the **Exclusions** tab, select the **Do not control excluded IP-addresses** check box.

   If this check box is selected, Kaspersky Embedded Systems Security for Windows doesn't scan inbound network traffic for excluded IP addresses.

   If this check box is cleared, Kaspersky Embedded Systems Security for Windows doesn't apply the exclusion list.

6. Specify the IP address and click **Add** button.
7. Click the **OK** button.

Configuring the Network Threat Protection task via the Web Plug-in

In this section, learn how to manage the Network Threat Protection task via the Web Plug-in interface.

General task settings

To configure the general settings of the Network Threat Protection task using the Web Console:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.
2. Click the policy name you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.
4. Select the **Real-time computer protection** section.
5. In the **Network Threat Protection** block, click the **Settings** button.

   The **Network Threat Protection** window opens.

6. Select the **General** tab.
7. In the **Operating mode** section select the processing mode:

   - **Pass-through**.

If this mode is selected, Kaspersky Embedded Systems Security for Windows scans inbound network traffic for activity that is typical of network attacks, but doesn't log events about detected activity and doesn't block network activity from the attacking computer.

For example, you can use this mode in case of a decrease in the protected device's performance.

- **Only inform about network attacks**.

  If this mode is selected, Kaspersky Embedded Systems Security for Windows scans inbound network traffic for activity that is typical of network attacks, logs events about detected activity, but doesn't block network activity from the attacking computer.

- **Block connections when attack is detected**.

  The check box enables or disables adding hosts showing activity typical of network attacks to the list of blocked hosts.

  If this mode is selected, Kaspersky Embedded Systems Security for Windows scans inbound network traffic for activity that is typical of network attacks, logs events about detected activity, and adds IP addresses of hosts showing activity typical of network attacks to the list of blocked hosts.

  You can view the list of blocked hosts in the Blocked Hosts storage.

  You can restore access to blocked hosts, and specify the number of days, hours, and minutes after which hosts regain access to network file resources after being blocked by configuring the Blocked Hosts storage settings.

  The mode is selected by default.

8. In the **MAC spoofing protection** block, select or clear the **Enable protection against MAC spoofing attacks** check box.

   A MAC address spoofing attack consists of changing the MAC address of a network device (network card). As a result, an attacker could redirect data sent to a device to another device and gain access to this data.

   If the check box is selected and the Network Threat Protection task mode is different from **Pass-through**, Kaspersky Embedded Systems Security for Windows scans incoming network traffic for actions that are typical of MAC address spoofing attacks and performs actions in accordance with the selected task mode for the Network Threat Protection task.

   If the check box is cleared or the **Pass-through** task mode is selected, Kaspersky Embedded Systems Security for Windows does not scan incoming network traffic for actions typical of MAC address spoofing attacks.

   By default, the check box is cleared.

9. Select or clear the **Don't stop traffic analysis when the task is not running** check box.

If this check box is selected, then even when the Network Threat Protection task is stopped, Kaspersky Embedded Systems Security for Windows scans inbound network traffic for activity that is typical of network attacks and blocks network activity from the attacking computer, depending on the selected task mode.

If this check box is cleared, when the Network Threat Protection task is stopped, Kaspersky Embedded Systems Security for Windows doesn't scan inbound network traffic for activity that is typical of network attacks.

By default, the check box is cleared.

10. Click the **OK** button.

Adding exclusions

To add exclusions for Network Threat Protection task, take the following steps:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.
2. Click the policy name you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.
4. Select the **Real-time computer protection** section.
5. Click the **Settings** button in the **Network Threat Protection** subsection.
6. On the **Exclusions** tab, select the **Do not control excluded IP-addresses** check box.

   If this check box is selected, Kaspersky Embedded Systems Security for Windows doesn't scan inbound network traffic for excluded IP addresses.

   If this check box is cleared, Kaspersky Embedded Systems Security for Windows doesn't apply the exclusion list.

7. Specify the IP address and click **Add** button.
8. Click the **OK** button.

Applications Launch Control

This section contains information about the Applications Launch Control task and how to configure it.

About the Applications Launch Control task

When running the Applications Launch Control task, Kaspersky Embedded Systems Security for Windows monitors user's attempts to start applications and allows or denies start of these applications. The Applications Launch Control task relies on the Default Deny principle, which means that any applications that are not allowed in the task settings will be blocked automatically.

You can allow applications to start using one of the following methods:

- Set allowing rules for trusted applications.
- Check trusted applications reputation in KSN on launch.

The task gives top priority to denying the start of applications. For example, if an application is prevented from starting by one of the blocking rules, the application start will be denied regardless of the trusted conclusion for KSN. At that, if the application is not trusted by the KSN services but is included in the scope of an allowing rule, the application start will be denied.

All attempts to start applications are recorded in the task log.

The Applications Launch Control task can operate in one of two modes:

- **Active**. Kaspersky Embedded Systems Security for Windows uses a set of rules to control the start of applications that fall within the scope of the Applications Launch Control rules. The scope of the Applications Launch Control rules is specified in the settings of this task. If an application falls within the scope of the Applications Launch Control rules, and the task settings do not satisfy any specified rule, the application launch will be denied.

  Launches of applications that do not fall within the scope of any rule specified in the Applications Launch Control task settings are denied regardless of the Applications Launch Control task settings.

  The **Applications Launch Control** task cannot be started in Active mode if no rules have been created or if there are more than 65,535 rules for one protected device.

- **Statistics only**. Kaspersky Embedded Systems Security for Windows does not use Applications Launch Control rules to allow or deny the start of applications. Instead, it only records information about application starts, rules satisfied by running applications, and actions that would have been performed if the task was running in **Active** mode. All applications are allowed to start. This mode is set by default.

  You can use this mode to create Applications Launch Control rules based on information recorded in the task log.

You can configure the Applications Launch Control task according to one of the following scenarios:

- Advanced configuration and application of applications launch control rules.
- Basic rule configuration and KSN usage for Applications Launch Control.

If operating system files fall within the scope of the Applications Launch Control task, we recommend that when creating Applications Launch Control rules you make sure that such applications are allowed by the newly created rules. Otherwise, the operating system may fail to start.

Kaspersky Embedded Systems Security for Windows also intercepts processes launched under the Windows Subsystem for Linux (except for scripts run from the UNIX™ shell, or command line interpreters). For such processes, the Applications Launch Control task applies the action defined by the current configuration. The Rule Generator for Applications Launch Control task detects application launches and generates corresponding rules for applications running under the Windows Subsystem for Linux.

About Applications Launch Control rules

How Applications Launch Control rules work

The operation of Applications Launch Control rules is based on the following components:

- Type of rule.

  Applications Launch Control rules can allow or deny the start of application. Accordingly, they are called *allowing* or *denying* rules. To create a list of allowing rules for Applications Launch Control, you can use the Rule Generator for generating allowing rules or use the Applications Launch Control task in **Statistics only** mode. You can also add allowing rules manually.

- User or group of users.

  Applications Launch Control rules can control the start of specified applications by a user and / or user group.

- Rule usage scope.

  Applications Launch Control rules can be applied to *executable files, scripts,* and *MSI packages*.

- Rule triggering criterion.

  Applications Launch Control rules control the launch of files that satisfy one or several of the criteria specified in the rule settings: signed by the specified *digital certificate*, matching the specified *SHA256 hash*, located at the specified *path*, and matching the specified *command line* arguments. You should select at least one option. Otherwise, the Application Launch Control rule is not added.

  If **Digital certificate** is set as the rule triggering criterion, the created rule controls the start of all trusted applications in the operating system. You can set stricter conditions for this criterion by selecting the following check boxes:

  - **Use subject**
  - **Use thumb**

  Thumbprints allow for the most restrictive triggering of application start rules based on a digital certificate, because a thumbprint uniquely identifies a digital certificate and cannot be forged, unlike the subject of a digital certificate.

You can specify exclusions for Applications Launch Control rules. Exclusions to Applications Launch Control rules are based on the same criteria used to trigger rules: digital certificate, SHA256 hash, and file path. Exclusions to Applications Launch Control rules may be required for certain allowing rules: for example, if you want to allow users to start applications from the C:\Windows path, while blocking launch of the Regedit.exe file.

If operating system files fall within the scope of the Applications Launch Control task, we recommend that when creating Applications Launch Control rules you make sure that such applications are allowed by the newly created rules. Otherwise, the operating system may fail to start.

Managing Applications Launch Control rules

You can perform the following actions with Applications Launch Control rules:

- Add rules manually.
- Generate and add rules automatically.
- Remove rules.
- Export rules to file.
- Check selected files for rules that allow execution of these files.
- Filter the rules in the list according to specified criterion.

About Software Distribution Control

Generating Applications Launch Control rules can be complicated if you also need to control software distribution on a protected device, for example, on protected devices where installed software is periodically automatically updated. In this case, the list of allowing rules must be updated after each software update for newly created files to be considered in the Applications Launch Control task settings. To simplify launch control in software distribution scenarios, you can use the Software Distribution Control subsystem.

A *software distribution package* (hereinafter referred to as "package") represents a software application to be installed on a protected device. Each package contains at least one application and may also contain individual files, updates, or even an individual command, in addition to applications, particularly when you are installing a software application or update.

The Software Distribution Control subsystem is implemented as an additional list of exclusions. When an installation package is added to the list, it becomes trusted. Unpacking is allowed for trusted packages, and automatic startup is allowed for applications installed or updated from trusted packages. The extracted files can inherit the trusted attribute of the primary distribution package. A *primary distribution package* is a package that has been added to the list of Software Distribution Control exclusions by a user and has become a trusted package.

Kaspersky Embedded Systems Security for Windows controls only full software distribution cycles. The application cannot correctly process the launch of files modified by a trusted package if, when the package is started for the first time, software distribution control is turned off or the Application Launch Control component is not installed.

Software distribution control is not available if the **Apply rules to executable files** check box is cleared in the Applications Launch Control task settings.

Software distribution cache

Kaspersky Embedded Systems Security for Windows uses a dynamically generated software distribution cache ("distribution cache") to establishes the relationship between trusted packages and files created during software distribution. When a package is first started, Kaspersky Embedded Systems Security for Windows detects all files created by the package during the software distribution process and stores file checksums and paths in the distribution cache. Then all files in the distribution cache are allowed to start by default.

You cannot review, clear or manually modify the distribution cache via the user interface. The cache is populated and controlled by Kaspersky Embedded Systems Security for Windows.

You can export the distribution cache to a configuration file (XML format) and clear the cache using command line options.

To export the distribution cache to a configuration file, execute the following command:

```
kavshell appcontrol /config /savetofile:<full path> /sdc
```

To clear the distribution cache, execute the following command:

```
kavshell appcontrol /config /clearsdc
```

Kaspersky Embedded Systems Security for Windows updates the distribution cache every 24 hours. If the checksum of a previously allowed file is changed, the application deletes the record for this file from the distribution cache. If the Applications Launch Control task is started in Active mode, subsequent attempts to start this file will be blocked. If the full path to the previously allowed file is changed, subsequent attempts to start this file will not be blocked, because the checksum is stored within the distribution cache.

Processing the extracted files

All files extracted from a trusted package inherit the trusted attribute upon first launch of the package. If you clear the check box after first launch, all files extracted from the package will retain the inherited attribute. To reset the inherited attribute on all extracted files, you need to clear the distribution cache and clear the **Allow the further distribution of programs created from this distribution package** check box before starting the trusted distribution package again.

Extracted files and packages created by a primary trusted distribution package inherit the trusted attribute when their checksums are added to the distribution cache when the software distribution package in the exclusion list is opened for the first time. Hence, the distribution package itself and all files extracted from this package will also be trusted. By default, the number of levels of inheritance of the trusted attribute is unlimited.

Extracted files will retain the trusted attribute after the operating system restarts.

The processing of files is configured in the Software Distribution Control settings by selecting or clearing the **Allow the further distribution of programs created from this distribution package** check box.

For example, if test.msi, a package containing several packages and applications, is added to the list of exclusions and the check box is selected, all packages and applications contained in the test.msi package can be unpacked and run, even if they contain other nested files. This scenario works for extracted files on all nested levels.

If you add a test.msi package to the exclusions list and clear the **Allow the further distribution of programs created from this distribution package** check box, the application will assign the trusted attribute only to the packages and executable files extracted directly from the primary trusted package (on the first level of nesting). The checksums of such files are stored in the distribution cache. All files on the second level of nesting and beyond will be blocked by the Default Deny principle.

Working with the Applications Launch Control rule list

The list of trusted packages of software distribution control subsystem is a list of exclusions, which amplifies, but does not replace the general list of applications launch control rules.

Denying applications launch control rules have the highest priority: trusted package decompression and start of new or modified files will be blocked, if these packages and files are affected by the applications launch control denying rules.

Software distribution control exclusions are applied both for trusted packages and files created or modified by these packages, if no denying rules in the applications launch control list are applied for those packages and files.

Using KSN conclusions

KSN conclusions that a file is untrusted have a higher priority than the Software Distribution Control exclusions. Unpacking of trusted packages and the launch of files created or modified by trusted packages will be blocked if a KSN conclusion has been received and indicates that such files are untrusted.

At that, after unpacking from a trusted package, all child files will be allowed to run regardless of KSN usage within the Applications Launch Control scope. At that, states of **Deny applications untrusted by KSN** and **Allow applications trusted by KSN** check boxes do not affect the operation of the **Allow the further distribution of programs created from this distribution package** check box.

About KSN usage for the Applications Launch Control task

To start the KSN Usage task, you must accept the Kaspersky Security Network Statement.

If KSN data about an application's reputation is used by the Applications Launch Control task, the KSN application reputation is considered a criterion for allowing or denying launch of that application. If KSN reports to Kaspersky Embedded Systems Security for Windows that an application is untrusted when the user attempts to launch the application, the application launch is denied. If KSN reports to Kaspersky Embedded Systems Security for Windows that the application is trusted when the user attempts to launch the application, the application launch is allowed. KSN can be used along with Applications Launch Control rules or as an independent criterion for denying launch of applications.

Using KSN conclusions as independent criterion for denying application launch

This scenario lets you securely control application launches on a protected device without requiring advanced configuration of the rule list.

You can apply KSN conclusions to Kaspersky Embedded Systems Security for Windows together with the only specified rule. The application will only allow the start of applications that are trusted in KSN or are allowed by a specified rule.

For such a scenario, we recommend that you set a rule allowing start of the application based on a digital certificate.

All other applications are denied in accordance with the Default Deny policy. Using KSN when no rules are applied protects a device from applications that KSN considers to be a threat.

Using KSN conclusions simultaneously with Applications Launch Control rules

When using KSN conclusions simultaneously with Applications Launch Control rules, the following conditions apply:

- Kaspersky Embedded Systems Security for Windows always denies launch of an application if it is included in the scope of at least one denying rule. If the application is considered trusted by KSN, the corresponding conclusion has a lower priority and is not considered; the application launch will still be denied. This lets you expand the list of blocked applications.

- Kaspersky Embedded Systems Security for Windows always denies the launch of an application if the launch of applications not trusted in KSN is prohibited and the application is not trusted in KSN. If an allowing rule is set for the application, it has a lower priority and is not considered; the application launch will still be denied. This protects the device from applications that KSN considers to be a threat but were not considered during initial configuration of the rules.

About the Rule Generator for Applications Launch Control

You can create lists of Applications Launch Control rules using Kaspersky Security Center tasks and policies simultaneously for all protected devices and groups of protected devices on the corporate network. The scenarios listed below are recommended if the corporate network does not have a reference machine and you are unable to create a list of allowing rules based on applications installed on the template machine.

You can run the Rule Generator for Applications Launch Control task locally via the Application Console to create a list of rules based on the applications running on a single protected device.

The Applications Launch Control component is installed with two preset allowing rules:

- Allowing rule for scripts and Windows Installer packages with a certificate trusted by the operating system.

- Allowing rule for executable files with a certificate trusted by the operating system.

You can create lists of Applications Launch Control rules on the side of Kaspersky Security Center in one of the following ways:

- Using a Rule Generator for Applications Launch Control group task.

  Under this scenario, a group task generates its own list of Applications Launch Control rules for each protected device on the network and saves those lists to an XML file in the specified shared folder. The XML file generated by the Rule Generator for Applications Launch Control task contains the allowing rules specified in task settings before the task starts. No rules will be created for applications that are not allowed to start in the specified task settings. The start of such applications is denied by default. You can then manually import the created list of rules into the Applications Launch Control task for the Kaspersky Security Center policy.

  You can configure the generated rules to be automatically imported into the list of rules for the Applications Launch Control task.

This scenario is recommended when you need to quickly create lists of Applications Launch Control rules. We recommend that you configure the scheduled launch of the Rule Generator for Applications Launch Control task only if the allowing rules usage scope includes folders and files you know to be safe.

Before using the Applications Launch Control task in the network, make sure that all protected devices have access to a shared folder. If the organization's policy does not provide for the use of a shared folder in the network, we recommend that you start the Rule Generator for Applications Launch Control task on a protected device in the test protected devices group or on a reference machine.

- Based on a report of task events generated in Kaspersky Security Center by the Applications Launch Control task running in **Statistics only** mode.

  Under this scenario, Kaspersky Embedded Systems Security for Windows does not deny the launch of applications. Instead, with Applications Launch Control running in the **Statistics only** mode, it reports all allowed and denied application launches across all network protected devices in the **Events** tab of the Administration Server node's workspace in the Kaspersky Security Center. Kaspersky Security Center uses the reports to generate a single list of events in which application launches were denied.

  You need to configure the task execution period so that all possible scenarios involving the protected devices and protected device groups, and at least one protected device restart are performed during the specified time period. After the end of the task execution period, you can import application launch data from the saved Kaspersky Security Center event report (TXT format) and generate Applications Launch Control allowing rules for such applications based on this data.

  This scenario is recommended if a corporate network includes a large number of protected devices of different type (with a different software installed).

- Based on denied application launch events received through Kaspersky Security Center, without creating and importing a configuration file.

  To use this feature, the Applications Launch Control task on the protected device must be running under an active Kaspersky Security Center policy. In this case, all events on the protected device are sent to the Administration Server.

We recommend that you update the list of rules when the set of applications installed on network protected devices changes (for example, when updates are installed or operating systems are reinstalled). We recommend that you generate an updated list of rules by running the Rule Generator for Applications Launch Control task or the Applications Launch Control task in **Statistics only** mode on protected devices in the test administration group. The test administration group includes the protected devices required to test the launch of new applications before they are installed on network protected devices.

XML files containing lists of allowing rules are created based on an analysis of tasks started on the protected device. To account for all applications used on the network when generating lists of rules you are advised to start the Rule Generator for Applications Launch Control task and the Applications Launch Control task in **Statistics only** mode on a template machine.

Before generating allowing rules based on the applications launched on a reference machine, make sure that the template machine is secure and there is no malware on it.

Before adding allowing rules, select one of the available rule application modes. The list of Kaspersky Security Center policy rules displays only rules specified by the policy, regardless of the rule application mode. The local rule list includes all applied rules — both local rules and rules added through a policy.

Default Applications Launch Control task settings

By default, the Applications Launch Control task has the settings described in the table below. You can change the values of these settings.

Default Applications Launch Control task settings

Setting	Default value	Description
Task mode.	**Statistics only**. The task records denied launch events and allowed launch events based on the set rules. Application launch is not actually denied.	You can select **Active** mode after the final list of rules is generated.
Repeat action taken for the first file launch on all the subsequent launches for this file	Not applied	You can repeat actions taken for the first file launch on all the subsequent launches for this file.
Deny the command interpreters launch with no command to execute	Not applied.	You can deny launch of command line interpreters with no command to execute.
Rules managing	**Add policy rules to the local rules**	You can select a mode in which rules specified in a policy are applied together with the rules on the protected device.
Rule usage scope	The task controls the launch of executable files, scripts, and MSI packages. The task also monitors loading of DLL modules.	You can specify the file types for which launch is controlled by rules.
KSN Usage	KSN application reputation data is not used.	You can use KSN application reputation data when running the Applications Launch Control task.
Automatically allow software distribution via applications and packages listed	Not applied.	You can allow software distribution using the installers and applications specified in the settings. By default, software distribution is only allowed using the Windows Installer service.
Always allow software distribution via Windows Installer	Applied. Can be changed only when the **Automatically allow software distribution via applications and packages listed** setting is enabled.	You can allow any software installation or update if the operations are performed via Windows Installer.
Always allow software distribution via SCCM using the Background Intelligent Transfer Service	Not applied. Can be changed only when the **Automatically allow software distribution via applications and packages listed** setting is enabled.	You can turn on or off automatic software distribution using the System Center Configuration Manager.
Task start	First run is not scheduled.	The Applications Launch Control task does not start automatically at start of Kaspersky

		Embedded Systems Security for Windows. You can start the task manually or configure a scheduled start.

Rule Generator for Applications Launch Control task default settings

Setting	Default value	Description
Prefix for allowing rules names	Identical to the name of the protected device on which Kaspersky Embedded Systems Security for Windows is installed.	You can change the prefix for names of allowing rules.
Allowing rules usage scope	The allowing rules usage scope includes the following file categories by default: • Files with the EXE extension located in the folders C:\Windows, C:\Program Files (x86) and C:\Program Files • MSI packages stored in the C:\Windows folder • Scripts stored in the C:\Windows folder The task also creates rules for all running applications, regardless of their location and format.	You can change the protection scope by adding or removing folder paths and specifying the types of files that will be allowed to launch by the automatically generated rules. You can also ignore running applications when creating allowing rules.
Criteria for generation of allowing rules	The digital certificate subject and thumbprint are used; rules are generated for all users and groups of users.	You can use the SHA256 hash when generating allowing rules. You can select a user and group of users for which allowing rules need to be automatically generated.
Actions upon task completion	Allowing rules are added to the list of Applications Launch Control rules; new rules are merged with existing rules; duplicate rules are removed.	You can add rules to the existing rules without merging them and without deleting duplicate rules, or replace existing rules with the new allowing rules, or configure export of the allowing rules to a file.
Task launch settings with permissions	The task is started under a system account.	You can allow the Rule Generator for Applications Launch Control task to start under a system account or using the permissions of a specified user.
Task start schedule	First run is not scheduled.	The Rule Generator for Applications Launch Control task does not start automatically when Kaspersky Embedded Systems Security for Windows starts. You can start the task manually or configure a scheduled start.

Managing Applications Launch Control via the Administration Plug-in

In this section, learn how to navigate the Administration Plug-In interface and configure task settings for one or all protected devices on the network.

Navigation

Learn how to navigate to the required task settings via the chosen interface.

Opening policy settings for the Applications Launch Control task

To open the Applications Launch Control task settings via the Kaspersky Security Center policy:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure the task.
3. Select the **Policies** tab.
4. Double-click the policy name you want to configure.
5. In the **Properties: <Policy name>** window that opens, select the **Local activity control** section.
6. Click the **Settings** button in the **Applications Launch Control** subsection.
   The **Applications Launch Control** window opens.

Configure the policy as required.

Opening the Applications Launch Control rules list

To open the Applications Launch Control rules list via the Kaspersky Security Center:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure the task.
3. Select the **Policies** tab.
4. Double-click the policy name you want to configure.
5. In the **Properties: <Policy name>** window that opens, select the **Local activity control** section.
6. Click the **Settings** button in the **Applications Launch Control** subsection.
   The **Applications Launch Control** window opens.
7. On the **General** tab, click the **Rules list** button.
   The **Applications Launch Control rules** window opens.

Configure the rules list as required.

Opening the Rule Generator for Applications Launch Control task wizard and properties

To start creating a Rule Generator for Applications Launch Control task:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure the task.
3. Open the **Tasks** tab.
4. Click the **New task** button.
   The **New Task Wizard** window opens.
5. Select the **Rule Generator for Applications Launch Control** task.
6. Click the **Next** button.
   The **Settings** window opens.

To configure the Rule Generator for Applications Launch Control task:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure the task.
3. Open the **Tasks** tab.
4. Double-click the task name in the list of Kaspersky Security Center tasks.
   The **Properties: Rule Generator for Applications Launch Control** window opens.

See the Configuring the Rule Generator for Applications Launch Control task section for details on configuring the task.

Configuring Applications Launch Control task settings

To configure general Applications Launch Control task settings:

1. Open the **Applications Launch Control** window.
2. On the **General** tab, select the following settings in the **Task mode** section:
   - In the **Task mode** drop-down list, specify the task mode.
   - Clear or select the **Repeat action taken for the first file launch on all the subsequent launches for this file** check box.
   - Clear or select the **Deny the command interpreters launch with no command to execute**.
3. In the **Rules managing** block, configure settings for applying rules:

a. Click the **Rules list** button to add allowing rules for the Applications Launch Control task.

> Kaspersky Embedded Systems Security for Windows does not recognize paths that contain slashes ("/"). Use backslash ("\") to enter the path correctly.

b. Select the mode for applying rules:

- **Replace local rules with policy rules**

  The application applies the rule list specified in the policy for centralized application launch control on a group of protected devices. Local rule lists cannot be created, edited, or applied.

- **Add policy rules to the local rules**

  The application applies the rule list specified in a policy together with local rule lists. You can edit the local rule lists using the Rule Generator for Applications Launch Control task.

4. In the **Rule usage scope** section, specify the following settings:

- Apply rules to executable files.
- Monitor loading of DLL modules.

> Controlling loading of DLL modules may affect the performance of the operating system.

- Apply rules to scripts and MSI packages.

5. In the **KSN Usage** group box, configure the following application launch settings:

- Deny applications untrusted by KSN.
- Allow applications trusted by KSN.
- Users and / or user groups allowed to launch applications trusted in KSN:

  a. In the context menu of the **Edit** button, select the method for adding users.

  The **Select user or user group** window opens.

  b. Select a user or user group.

  c. Click the **OK** button.

6. On the **Software Distribution Control** tab, configure the settings for software distribution control.

7. On the **Task management** tab, configure the task start schedule settings.

8. Click the **OK** button in the **Applications Launch Control** window.

Kaspersky Embedded Systems Security for Windows immediately applies the new settings to the running task. Information about the date and time when the settings were modified, and the values of task settings before and after modification, are saved in the system audit log.

Configuring Software Distribution Control

To add a trusted distribution package via the Administration Plug-in:

1. Open the **Applications Launch Control** window.

2. On the **Software Distribution Control** tab, select the **Automatically allow software distribution via applications and packages listed** check box.

   You can select the **Automatically allow software distribution via applications and packages listed**, if the **Applications Launch Control** check box in the **Apply rules to executable files** tab is selected in the **General** task settings.

3. Clear the **Always allow software distribution via Windows Installer** check box if required.

   Clearing the **Always allow software distribution via Windows Installer** check box is only recommended if it is absolutely necessary. Turning off this function may cause issues with updating operating system files and also prevent the launch of files extracted from a distribution package.

4. If required, select the **Always allow software distribution via SCCM using the Background Intelligent Transfer Service** check box.

   The application controls the software distribution cycle on the protected device — from package delivery to installation or update. The application does not control processes if any stage of distribution was performed before installation of the application on the protected device.

5. To create the allow list or to edit the existing list of trusted distribution packages, click **Change packages list** and select one of the following methods in the window that appears:

   - **Add one distribution package**.

     a. Click the **Browse** button.

     b. Select the executable file or distribution package.

     The **Trusting criteria** block is automatically populated with data about the selected file.

     c. Clear or select the **Allow the further distribution of programs created from this distribution package** check box.

     d. Select one of two available options for criteria to use to determine whether a file or distribution package is trusted:

     - **Use digital certificate**
     - **Use SHA256 hash**

   - **Add several packages by hash**

     You can select an unlimited number of executable files and distribution packages, and add them to the list all at the same time. Kaspersky Embedded Systems Security for Windows examines the hash and allows the operating system to launch the specified files.

- **Change selected package**

  Use this option to select a different executable file or distribution package, or to change the trust criteria.

- **Import distribution packages list from file**.

  In the **Open** window, specify the configuration file containing a list of trusted distribution packages.

If you create a trusted distribution package based on an executable file and you added a process in the Trusted Zone settings based on that same executable file and made it trusted for the Applications Launch Control task, the Trusted Zone settings have a higher priority. Kaspersky Embedded Systems Security for Windows blocks this executable file from starting, but considers the executable file's process to be trusted.

6. If you want to remove a previously added application or distribution package from the trusted list, click the **Delete distribution packages** button. Extracted files will be allowed to run.

   To prevent extracted files from starting, uninstall the application on the protected device or create a denying rule in the Applications Launch Control task settings.

7. Click the **OK** button.

The specified settings are saved.

Configuring a Rule Generator for Applications Launch Control task

To configure the Rule Generator for Applications Launch Control task:

1. Open the **Properties: Rule Generator for Applications Launch Control** window.
2. In the **Notification** section, configure the task event notification settings.

   For detailed information on configuring settings in this section, see *Kaspersky Security Center Help*.

3. In the **Settings** section, you can configure the following settings:

   - Specify prefix for rule names.
   - Select how to create allowing rules:
     - **Create allowing rules based on running applications**
     - **Create allowing rules for applications from the folders**

4. In the **Options** section, you can specify actions to perform while creating allowing rules for applications launch control:

   - **Use digital certificate**
   - **Use digital certificate subject and thumbprint**

- If the certificate is missing, use
  - **SHA256 hash**. The checksum of the file used to generate the rule is set as a criterion for triggering the allowing rule for Applications Launch Control. The application will allow start of programs launched using files with the specified checksum.
  - **path to file**. The path to the file used to generate the rule is set as a criterion for triggering the allowing rule for Applications Launch Control. The application will now allow start of programs launched using files located in the folders specified in the **Create allowing rules for applications from the folders** table in the **Settings** section.
- Use SHA256 hash
- Generate rules for user or group of users.

You can configure settings for configuration files with lists of allowing rules for Device Control and Applications Launch Control. Kaspersky Embedded Systems Security for Windows creates these lists when the task is complete.

5. Configure the task schedule in the **Schedule** section (you can configure a schedule for all task types except Rollback of Database Update).
6. In the **Account** section, specify the account whose rights will be used to run the task.
7. If required, specify the objects to exclude from the task scope in the **Exclusions from task scope** section.

   For detailed information on configuring settings in these sections, see *Kaspersky Security Center Help*.
8. Click the **OK** button in the **Properties: <Task name>** window.

   The newly configured group task settings are saved.

Configuring Applications Launch Control rules via the Kaspersky Security Center

Learn how to generate a list of rules based on various criteria or manually create allowing or denying rules using the Application Launch Control task.

Adding an Applications Launch Control rule

To add an Applications Launch Control rule using the Administration Plug-in:

1. Open the **Applications Launch Control rules** window.
2. Click the **Add** button.
3. In the context menu of the button, select **Add one rule**.

   The **Rule settings** window opens.

4. Specify the following settings:

a. In the **Name** field, enter the name of the rule.

b. In the **Type** drop-down list, select the rule type:

- **Allowing**, if you want the rule to allow launch of applications in accordance with the criteria specified in the rule settings.
- **Denying**, if you want the rule to block launch of applications in accordance with the criteria specified in the rule settings.

c. In the **Scope** drop-down list, select the type of files whose execution will be controlled by the rule:

- **Executable files**, if you want the rule to control launch of executable files.
- **Scripts and MSI packages**, if you want the rule to control launch of scripts and MSI packages.

d. In the **User or user group** field, specify the users who will or will not be allowed to start programs based on the type of rule.

1. In the context menu of the **Browse** button, select the method for adding trusted users.

   The **User or user group selection** window opens.

2. Select a user or user group.

3. Click the **OK** button.

e. If you want to take the values of the rule-triggering criteria listed in the **Rule triggering criterion** block from a file, do the following:

1. Click the **Set rule triggering criterion from file properties** button.

   The standard Microsoft Windows **Open** window opens.

2. Select the file.

3. Click the **Open** button.

   The value of the criteria in the file are displayed in the fields in the **Rule triggering criterion** block. The criterion for which data are available in the file properties is selected by default.

f. In the **Rule triggering criterion** group box, select one or several of the following options as applicable:

- **Digital certificate**, if you want the rule to control the launch of applications launched using files signed with a digital certificate:
  - Select the **Use subject** check box if you want the rule to control the launch of files signed with a digital certificate only with the specified subject.
  - Select the **Use thumb** check box if you want the rule to only control the launch of files signed with a digital certificate with the specified thumbprint.
- **SHA256 hash**, if you want the rule to control the launch of programs launched using files whose checksum matches the one specified.
- **Path to file**, if you want the rule to control the launch of programs launched using files located at the specified path.

- **Command line** if you want the rule to control the start of programs launched using the arguments specified in the command line field. The field is enabled after you select the **Path to file** option. You can use ? and * characters as a mask when specifying the command line arguments for launched processes as a criterion.

Kaspersky Embedded Systems Security for Windows does not recognize paths that contain slashes ("/"). Use backslash ("\") to enter the path correctly.

When specifying the objects, you can use ? and * characters as file masks.

You should select at least one option. Otherwise, the Application Launch Control rule is not added.

g. If you want to add rule exclusions:

1. In the **Exclusions from rule** section, click the **Add** button.

   The **Exclusion from rule** window opens.

2. In the **Name** field, enter the name of the exclusion.

3. Specify the settings for exclusion of application files from the Applications Launch Control rule. You can fill out the settings fields from the file properties by clicking the **Set exclusion based on file properties** button.

   - **Digital certificate**
   - **Use subject**
   - **Use thumb**
   - **SHA256 hash**
   - **Path to file**

4. Click the **OK** button.

5. If necessary, repeat steps (i)-(iv) to add additional exclusions.

5. Click the **OK** button in the **Rule settings** window.

The created rule is displayed in the list in the **Applications Launch Control rules** window.

Enabling the Default Allow mode

Default Allow mode allows all applications to start if they are not blocked by rules or by a conclusion from KSN that they are not trusted. Default Allow mode can be enabled by adding specific allowing rules. You can enable Default Allow for only scripts or for all executable files.

To add a Default Allow rule:

1. Open the **Applications Launch Control rules** window.

2. Click the **Add** button and, in the button's context menu, select **Add one rule**.

   The **Rule settings** window opens.

3. In the **Name** field, enter the name of the rule.

4. In the **Type** drop-down list, select the **Allowing** rule type.

5. In the **Scope** drop-down list, select the type of files whose execution will be controlled by the rule:

   - **Executable files**, if you want the rule to control launch of executable files.
   - **Scripts and MSI packages**, if you want the rule to control launch of scripts and MSI packages.

6. In the **Rule triggering criterion** group box, select the **Path to file** option.

7. Enter the following mask: `?:\`

8. Click the **Rule settings** button in the **OK** window.

Kaspersky Embedded Systems Security for Windows applies the Default Allow mode.

Creating allowing rules for applications launch control from Kaspersky Security Center events

To create allowing rules for applications launch control from Kaspersky Security Center events:

1. Open the Applications Launch Control rules window.

2. Click the **Add** button.

3. In the button's context menu, select **Create allowing rules for applications from Kaspersky Security Center events**.

4. Select the principle for adding the rules to the list of previously created Application Launch Control rules:

   - **Add to existing rules**, if you want to add the imported rules to the list of existing rules. Rules with identical settings are duplicated.
   - **Replace existing rules**, if you want to replace the existing rules with the imported rules.
   - **Merge with existing rules**, if you want to add the imported rules to the list of existing rules. Rules with identical settings are not added; the rule is added if at least one rule parameter is unique.

   The **Generating of the Applications Launch Control rules** window opens.

5. Select the event types based on which the application will create applications launch control rules:

   - **Statistics only mode: application launch denied**.
   - **Application launch denied**.

6. Select the time period from the **Request events that were generated within the period** drop-down list.

7. If necessary, in the **Use events generated for a group of managed devices** field, enter the name or a fragment of the name of the group of devices managed by Kaspersky Security Center whose events will be the basis for creating applications launch control rules.

8. Clear or select the **Prioritize the use of hash when generating rules** check box.

   If the check box is selected, Kaspersky Embedded Systems Security for Windows uses the checksum of the file to generate the rule when both the checksum and the certificate of the file are available.

   If the check box is cleared, Kaspersky Embedded Systems Security for Windows uses the digital certificate of the file to generate the rule when both the checksum and the certificate of the file are available.

9. Click the **Generate rules** button.

10. Click the **Save** button in the **Applications Launch Control rules** window.

    The rule list in the Applications Launch Control task will be populated with new rules generated based on system data from the protected device with the Kaspersky Security Center Administration Console installed.

    Rules with the same hash are not added, because all rules in the list must be unique.

Importing rules from a Kaspersky Security Center report on blocked applications

You can import data on blocked application launches from a report generated in Kaspersky Security Center after the Applications Launch Control task is run in **Statistics only** mode and use this data to generate a list of Applications Launch Control allowing rules in the policy being configured.

When generating a report on events occurring during the Applications Launch Control task, you can keep track of the applications whose launch is blocked.

When importing data from a report on blocked applications into policy settings, make sure that the list you are using contains only applications whose launch you want to allow.

To specify Applications Launch Control allowing rules for a group of protected devices based on a blocked applications report from Kaspersky Security Center:

1. Open the **Applications Launch Control** window.

2. In the **Task mode** block, select **Statistics only** mode.

3. In the policy properties in the **Event notification** section, make sure that:

   - For **Critical** events, the task log retention period for **Application launch denied** events exceeds the planned period for running the task in **Statistics only** mode (the default value is 30 days).

   - For events with an importance level of **Warning**, the task log retention period for **Statistics only mode: application launch denied** events exceeds the planned period for running the task in **Statistics only** mode (the default value is 30 days).

When the retention period for events elapses, information about the logged events is deleted and is not reflected in the report file. Before running the Applications Launch Control task in **Statistics only** mode, make sure that the task run time does not exceed the configured period for the specified events.

4. When the task has finished, export the logged events to a TXT file:

   a. In the workspace of the **Administration Server** node in Kaspersky Security Center, select the **Events** tab.

   b. Click the **Create a selection** button to create a selection of events based on the Blocked criterion to view the applications whose start will be blocked by the Applications Launch Control task.

   c. In the results pane of the selection, click **Export events to file** to save the blocked application starts report to a TXT file.

Before importing and applying the generated report in a policy, make sure that the report only contains data on the applications whose start you want to allow.

5. Import data on blocked application starts into the Applications Launch Control task. To do so, in the policy properties in the Applications Launch Control task settings:

   a. On the **General** tab, click the **Rules list** button.

      The **Applications Launch Control rules** window opens.

   b. Click the **Add** button and, in the button's context menu, select **Import data of blocked applications from Kaspersky Security Center report**.

   c. Select the principle for adding rules from the list created based on a Kaspersky Security Center report to the list of previously configured Applications Launch Control rules:

      - **Merge with existing rules**, if you want to add the imported rules to the list of existing rules. Rules with identical settings are not duplicated. If at least one rule setting is unique, the rule is added.
      - **Add to existing rules**, if you want to add the imported rules to the list of existing rules. Rules with identical settings are duplicated.
      - **Replace existing rules**, if you want to replace the existing rules with the imported rules.

   d. In the standard Microsoft Windows window that opens, select the TXT file to which events from the blocked application launch report have been exported.

   e. Click the **Save** button in the **Applications Launch Control rules** window.

Rules created based on the Kaspersky Security Center report on blocked applications are added to the list of Applications Launch Control rules.

Importing Applications Launch Control rules from an XML file

You can import reports generated by the Rule Generator for Applications Launch Control group task and apply them as a list of allowing rules in the policy you are configuring.

When the Rule Generator for Applications Launch Control group task finishes, the application exports the created allowing rules into XML files saved in the specified shared folder. Each file with a rule list is created by analyzing files executed and applications launched on each separate protected device on the corporate network. The lists contain allowing rules for files and applications whose type matches the type specified in the Rule Generator for Applications Launch Control group task.

To specify Applications Launch Control allowing rules for a group of protected devices based on an automatically generated list of allowing rules:

1. On the **Tasks** tab in the detail pane of the group of protected devices you are configuring, create a Rule Generator for Applications Launch Control group task or select an existing task.

2. In the properties of the created Rule Generator for Applications Launch Control group task or in the task wizard, specify the following settings:

   - In the **Notification** section, configure the settings for saving the task execution report.

     For detailed information on configuring settings in this section, see *Kaspersky Security Center Help*.

   - In the **Settings** section, specify the types of applications whose start will be allowed by the rules that are created. You can edit the set of folders containing allowed applications: exclude default folders from the task scope or add new folders manually.

   - In the **Options** section, specify the operations to be performed by the task while it is running and after it is finished. Specify the rule-generating criterion and the name of the file to which the generated rules will be exported.

   - In the **Schedule** section, configure the task start schedule settings.

   - In the **Account** section, specify the user account under which the task will be executed.

   - In the **Exclusions from task scope** section, specify the groups of protected devices to be excluded from the task scope.

     Kaspersky Embedded Systems Security for Windows does not create allowing rules for applications launched on excluded protected devices.

3. On the **Tasks** tab on the detail pane of the group of protected devices being configured, in the list of group tasks select the Rule Generator for Applications Launch Control task that you have created, and click the **Start** button to start the task.

   When the task is finished, the automatically generated lists of allowing rules are saved in XML files in a shared folder.

   Before using the Applications Launch Control task in the network, make sure that all protected devices have access to a shared folder. If the organization's policy does not provide for the use of a shared folder in the network, we recommend that you start the Rule Generator for Applications Launch Control task on a protected device in the test protected devices group or on a reference machine.

4. To add the generated lists of allowing rules to the Applications Launch Control task:

   a. Open the **Applications Launch Control rules** window.

b. Click the **Add** button and in the list that opens select **Import rules from XML file**.

c. Select the principle for adding the automatically generated allowing rules to the list of previously created Applications Launch Control rules:

- **Merge with existing rules**, if you want to add the imported rules to the list of existing rules. Rules with identical settings are not duplicated. If at least one rule setting is unique, the rule is added.
- **Add to existing rules**, if you want to add the imported rules to the list of existing rules. Rules with identical settings are duplicated.
- **Replace existing rules**, if you want to replace the existing rules with the imported rules.

d. In the standard Microsoft Windows window that opens, select XML files created after completion of the Rule Generator for Applications Launch Control group task.

e. Click the **Save** button in the **Applications Launch Control rules** window.

5. If you want to apply the created rules to control the launch of application, in the policy in the properties of the Applications Launch Control task, select the **Active** mode for the task.

Allowing rules automatically generated based on task runs on each separate protected device are applied to all network protected devices covered by the policy being configured. On these protected devices, the application will allow the launch of only those applications for which allowing rules have been created.

Checking application launches

Before applying the configured Applications Launch Control rules, you can test any application to determine which Applications Launch Control rules are triggered by that application.

By default, Kaspersky Embedded Systems Security for Windows denies the launch of applications whose launch is not allowed by a single rule. To avoid the denial of the launch of important applications, you need to create allowing rules for them.

If the launch of an application is controlled by several rules of different types, denying rules are given priority: the launch of an application will be denied if it falls under even one denying rule.

To test Applications Launch Control rules:

1. Open the **Applications Launch Control rules** window.
2. In the window that opens, click the **Show rules for the file** button.

   The standard Microsoft Windows window opens.
3. Select the file whose start control you want to test.

The path to the specified file is displayed in the search field. The list contains all rules that will be triggered when the selected file is started.

Creating a Rule Generator for Applications Launch Control task

To create and configure the Rule Generator for Applications Launch Control task settings:

1. Open the **Settings** window in the New Task Wizard.
2. Configure the following settings:
   - Specify Prefix for rule names.
   - Configure the allowing rules usage scope.
3. Click the **Next** button.
4. Specify the actions that must be performed by Kaspersky Embedded Systems Security for Windows:
   - when generating allowing rules
   - upon task completion
5. In the **Schedule** window, specify the task start schedule settings.
6. Click the **Next** button.
7. In the **Selecting an account to run the task** window, specify the account you want to use.
8. Click the **Next** button.
9. Enter the task name.
10. Click the **Next** button.

    The task name should be no longer than 100 characters and cannot contain the following symbols: " * < > & \ : |

    The **Finish creating the task** window opens.
11. Click the **Finish** button to finish creating the task.

To configure an existing rule in Kaspersky Security Center,

open the **Properties: Rule Generator for Applications Launch Control** window and configure the settings as described above.

Information about the date and time when the settings were modified, and the values of task settings before and after modification, are saved in the system audit log.

Restricting the task usage scope

To restrict the scope of the Rule Generator for Applications Launch Control task:

1. Open the **Properties: Rule Generator for Applications Launch Control** window.
2. Select how to create allowing rules:

- Create allowing rules based on running applications
- Create allowing rules for applications from the folders

3. Click the **OK** button.

The specified settings are saved.

Actions to perform during automatic rule generation

To configure the actions that Kaspersky Embedded Systems Security for Windows while the Rule Generator for Applications Launch Control task is running:

1. Open the **Properties: Rule Generator for Applications Launch Control** window.
2. Open the **Options** tab.
3. In the **While generating allowing rules** block, configure the following settings:
   - Use digital certificate
   - Use digital certificate subject and thumbprint
   - If the certificate is missing, use
     - **SHA256 hash**. The checksum of the file used to generate the rule is set as a criterion for triggering the allowing rule for Applications Launch Control. The application will allow start of programs launched using files with the specified checksum.
     - **path to file**. The path to the file used to generate the rule is set as a criterion for triggering the allowing rule for Applications Launch Control. The application will now allow start of programs launched using files located in the folders specified in the **Create allowing rules for applications from the folders** table in the **Settings** section.
   - Use SHA256 hash
   - Generate rules for user or group of users.
4. Click the **OK** button.

The specified settings are saved.

Actions to perform upon completion of automatic rule generation

To configure the actions to be taken by Kaspersky Embedded Systems Security for Windows after the Rule Generator for Applications Launch Control task is finished:

1. Open the **Properties: Rule Generator for Applications Launch Control** window.
2. Open the **Options** tab.
3. In the **After task completes** block, configure the following settings:

- Add allowing rules to the list of Applications Launch Control rules.
- Principle of adding.
- **Export allowing rules to file**.
- Add protected device details to file name.

4. Click the **OK** button.

The specified settings are saved.

Managing Applications Launch Control via the Application Console

In this section, learn how to navigate the Application Console interface and configure task settings on a protected device.

Navigation

Learn how to navigate to the required task settings via the chosen interface.

Opening the Applications Launch Control task settings

To open the Applications Launch Control general task settings via the Application Console:

1. In the Application Console tree, expand the **Computer Control** node.
2. Select the **Applications Launch Control** child node.
3. In the details pane of the **Applications Launch Control** child node, click the **Properties** link.
   The **Task settings** window appears.

Opening the Applications Launch Control rules window

To open the Applications Launch Control rule list via the Application Console:

1. In the Application Console tree, expand the **Computer Control** node.
2. Select the **Applications Launch Control** child node.
3. In the results pane of the **Applications Launch Control** node, click the **Applications Launch Control rules** link.
   The **Applications Launch Control rules** window opens.
4. Configure the rules list as required.

Opening the Rule Generator for Applications Launch Control task settings

To configure the Rule Generator for Applications Launch Control task:

1. In the Application Console tree, expand the **Automated rule generators** node.
2. Select the **Rule Generator for Applications Launch Control** child node.
3. In the results pane of the **Rule Generator for Applications Launch Control** child node, click the **Properties** link.
   The **Task settings** window appears.
4. Configure the task as required.

Configuring Applications Launch Control task settings

To configure general Applications Launch Control task settings:

1. Open the **Task settings** window.
2. Configure the following task settings:
   - On the **General** tab:
     - Applications Launch Control task mode.
     - Rule usage scope in the task.
     - KSN Usage.
   - Software Distribution Control settings on the **Software Distribution Control** tab.
   - Task start schedule settings on the **Schedule** and **Advanced** tabs.
3. Click the **OK** button in the **Task settings** window.
   The modified settings are saved.

Kaspersky Embedded Systems Security for Windows immediately applies the new settings to the running task. Information about the date and time when the settings were modified, and the values of task settings before and after modification, are saved in the system audit log.

Selecting the mode of the Applications Launch Control task

To configure the mode of the Applications Launch Control task:

1. Open the **Task settings** window.
2. On the **General** tab, in the **Task mode** drop-down list, specify the task mode.

3. Clear or select the **Repeat action taken for the first file launch on all the subsequent launches for this file** check box.

   Kaspersky Embedded Systems Security for Windows creates a new list of cached events every time the Applications Launch Control task settings are modified. This means that Applications Launch Control is performed according to the current security settings.

4. Clear or select the **Deny the command interpreters launch with no command to execute**.

5. Click the **OK** button in the **Task settings** window.

The specified settings are saved.

All attempts to start applications are recorded in the task log.

Configuring the scope of the Applications Launch Control task

To define the scope of the Applications Launch Control task:

1. Open the **Task settings** window.

2. On the **General** tab, in the **Rule usage scope** block, specify the following settings:

   - **Apply rules to executable files**
   - **Monitor loading of DLL modules**

     Controlling loading of DLL modules may affect the performance of the operating system.

   - **Apply rules to scripts and MSI packages**

3. Click the **OK** button in the **Task settings** window.

The specified settings are saved.

Configuring KSN usage

To configure the use of KSN services for the Applications Launch Control task:

1. Open the **Task settings** window.

2. On the **General** tab, in the **KSN Usage** block, specify the settings for use of KSN services:

   - If necessary, select the **Deny applications untrusted by KSN** check box.
   - If necessary, select the **Allow applications trusted by KSN** check box.

- If the **Allow applications trusted by KSN** check box is selected, indicate the users and/or groups of users allowed to start applications trusted in KSN. To do this, perform the following actions:

  a. Click the **Edit** button.

  The standard Microsoft Windows **Select users or groups** window opens.

  > By default, access to programs trusted in KSN is allowed to all users.

  b. Specify the list of users and/or user groups.

  c. Click the **OK** button.

3. Click the **OK** button in the **Task settings** window.

The specified settings are saved.

Configuring Software Distribution Control

To add a trusted distribution package via the Application Console:

1. Open the Task settings window.
2. On the **Software Distribution Control** tab, select the **Automatically allow software distribution via applications and packages listed** check box.

   > You can select the **Automatically allow software distribution via applications and packages listed**, if the **Applications Launch Control** check box in the **Apply rules to executable files** tab is selected in the **General** task settings.

3. Clear the **Always allow software distribution via Windows Installer** check box if required.

   > Clearing the **Always allow software distribution via Windows Installer** check box is only recommended if it is absolutely necessary. Turning off this function may cause issues with updating operating system files and also prevent the launch of files extracted from a distribution package.

4. If required, select the **Always allow software distribution via SCCM using the Background Intelligent Transfer Service** check box.

   > The application controls the software distribution cycle on the protected device — from package delivery to installation or update. The application does not control processes if any stage of distribution was performed before installation of the application on the protected device.

5. To create the allow list or to edit the existing list of trusted distribution packages, click **Change packages list** and select one of the following methods in the window that appears:

   - **Add one distribution package**.

     a. Click the **Browse** button.

b. Select the executable file or distribution package.

The **Trusting criteria** block is automatically populated with data about the selected file.

c. Clear or select the **Allow the further distribution of programs created from this distribution package** check box.

d. Select one of two available options for criteria to use to determine whether a file or distribution package is trusted:

- **Use digital certificate**
- **Use SHA256 hash**

- **Add several packages by hash**

  You can select an unlimited number of executable files and distribution packages, and add them to the list all at the same time. Kaspersky Embedded Systems Security for Windows examines the hash and allows the operating system to launch the specified files.

- **Change selected package**

  Use this option to select a different executable file or distribution package, or to change the trust criteria.

- Import distribution packages list from file.

  In the **Open** window, specify the configuration file containing a list of trusted distribution packages.

If you create a trusted distribution package based on an executable file and you added a process in the Trusted Zone settings based on that same executable file and made it trusted for the Applications Launch Control task, the Trusted Zone settings have a higher priority. Kaspersky Embedded Systems Security for Windows blocks this executable file from starting, but considers the executable file's process to be trusted.

6. If you want to remove a previously added application or distribution package from the trusted list, click the **Delete distribution packages** button. Extracted files will be allowed to run.

   To prevent extracted files from starting, uninstall the application on the protected device or create a denying rule in the Applications Launch Control task settings.

7. Click the **OK** button.

The specified settings are saved.

Configuring Applications Launch Control rules

Learn how to generate, import and export a list of rules, or manually create allowing or denying rules using the Application Launch Control task.

Adding an Applications Launch Control rule

To add an Applications Launch Control rule using the Application Console:

1. Open the **Applications Launch Control rules** window.
2. Click the **Add** button.
3. In the context menu of the button, select **Add one rule**.

   The **Rule settings** window opens.
4. Specify the following settings:

   a. In the **Name** field, enter the name of the rule.

   b. In the **Type** drop-down list, select the rule type:

   - **Allowing**, if you want the rule to allow launch of applications in accordance with the criteria specified in the rule settings.
   - **Denying**, if you want the rule to block launch of applications in accordance with the criteria specified in the rule settings.

   c. In the **Scope** drop-down list, select the type of files whose execution will be controlled by the rule:

   - **Executable files**, if you want the rule to control launch of executable files.
   - **Scripts and MSI packages**, if you want the rule to control launch of scripts and MSI packages.

   d. In the **User or user group** field, specify the users who will or will not be allowed to start programs based on the type of rule.

      1. In the context menu of the **Browse** button, select the method for adding trusted users.

         The **User or user group selection** window opens.
      2. Select a user or user group.
      3. Click the **OK** button.

   e. If you want to take the values of the rule-triggering criteria listed in the **Rule triggering criterion** block from a file, do the following:

      1. Click the **Set rule triggering criterion from file properties** button.

         The standard Microsoft Windows **Open** window opens.
      2. Select the file.
      3. Click the **Open** button.

         The value of the criteria in the file are displayed in the fields in the **Rule triggering criterion** block. The criterion for which data are available in the file properties is selected by default.

   f. In the **Rule triggering criterion** group box, select one or several of the following options as applicable:

- **Digital certificate**, if you want the rule to control the launch of applications launched using files signed with a digital certificate:
  - Select the **Use subject** check box if you want the rule to control the launch of files signed with a digital certificate only with the specified subject.
  - Select the **Use thumb** check box if you want the rule to only control the launch of files signed with a digital certificate with the specified thumbprint.
- **SHA256 hash**, if you want the rule to control the launch of programs launched using files whose checksum matches the one specified.
- **Path to file**, if you want the rule to control the launch of programs launched using files located at the specified path.
  - **Command line** if you want the rule to control the start of programs launched using the arguments specified in the command line field. The field is enabled after you select the **Path to file** option. You can use ? and * characters as a mask when specifying the command line arguments for launched processes as a criterion.

> Kaspersky Embedded Systems Security for Windows does not recognize paths that contain slashes ("/"). Use backslash ("\") to enter the path correctly.

> When specifying the objects, you can use ? and * characters as file masks.

You should select at least one option. Otherwise, the Application Launch Control rule is not added.

g. If you want to add rule exclusions:

1. In the **Exclusions from rule** section, click the **Add** button.

   The **Exclusion from rule** window opens.

2. In the **Name** field, enter the name of the exclusion.

3. Specify the settings for exclusion of application files from the Applications Launch Control rule. You can fill out the settings fields from the file properties by clicking the **Set exclusion based on file properties** button.
   - Digital certificate
   - Use subject
   - Use thumb
   - SHA256 hash
   - Path to file

4. Click the **OK** button.

5. If necessary, repeat steps (i)-(iv) to add additional exclusions.

5. Click the **OK** button in the **Rule settings** window.

The created rule is displayed in the list in the **Applications Launch Control rules** window.

Enabling the Default Allow mode

Default Allow mode allows all applications to start if they are not blocked by rules or by a conclusion from KSN that they are not trusted. Default Allow mode can be enabled by adding specific allowing rules. You can enable Default Allow for only scripts or for all executable files.

To add a Default Allow rule:

1. Open the **Applications Launch Control rules** window.
2. Click the **Add** button.
3. In the context menu of the button, select **Add one rule**.

   The **Rule settings** window opens.
4. In the **Name** field, enter the name of the rule.
5. In the **Type** drop-down list, select the **Allowing** rule type.
6. In the **Scope** drop-down list, select the type of files whose execution will be controlled by the rule:
   - **Executable files**, if you want the rule to control launch of executable files.
   - **Scripts and MSI packages**, if you want the rule to control launch of scripts and MSI packages.
7. In the **Rule triggering criterion** group box, select the **Path to file** option.
8. Enter the following mask: `?:\`
9. Click the **Rule settings** button in the **OK** window.

Kaspersky Embedded Systems Security for Windows applies the Default Allow mode.

Creating allowing rules from Applications Launch Control task events

To create a configuration file that contains allowing rules generated from Applications Launch Control task events:

1. Start the Applications Launch Control task in **Statistics only** mode to record information about all applications launches on a protected device in the task log.
2. After the task finishes running in **Statistics only** mode, open the task log by clicking the **Open task log** button in the **Management** block of the **Applications Launch Control** node's detail pane.
3. In the **Logs** window click the **Generate rules based on events**.

Kaspersky Embedded Systems Security for Windows will generate an XML configuration file containing a rule list based on events of the Applications Launch Control task in **Statistics only** mode. You can apply this rule list in the Applications Launch Control task.

Before applying the rule list generated from the logged task events, we recommend that you review and manually process the list to be certain that the launch of critical files (for example, system files) is allowed by the specified rules.

All task events are recorded in the task log regardless of the task mode. You can generate a configuration file with a rule list based on the log created while the task is running in **Active** mode. This scenario is not recommended except for urgent cases, because a final rule list must be generated before the task is run in **Active** mode in order to make it efficient.

Exporting Applications Launch Control rules

To export Applications Launch Control rules to a configuration file:

1. Open the **Applications Launch Control rules** window.
2. Click the **Export to a file** button.

   The standard Microsoft Windows window opens.
3. In the window that opens, specify the file to which you want to export the rules. If no such file exists, it will be created. If a file with the specified name already exists, its contents will be overwritten when the rules are exported.
4. Click the **Save** button.

The rule settings will be exported to the specified file.

Importing Applications Launch Control rules from an XML file

To import Applications Launch Control rules:

1. Open the **Applications Launch Control rules** window.
2. Click the **Add** button.
3. In the context menu of the button, select **Import rules from XML file**.
4. Specify the method for adding the imported rules. To do so, select one of the options from the context menu of the **Import rules from XML file** button:

   - **Add to existing rules**, if you want to add the imported rules to the list of existing rules. Rules with identical settings are duplicated.
   - **Replace existing rules**, if you want to replace the existing rules with the imported rules.
   - **Merge with existing rules**, if you want to add the imported rules to the list of existing rules. Rules with identical settings are not added; the rule is added if at least one rule parameter is unique.

   The standard Microsoft Windows **Open** window opens.
5. In the **Open** window, select the XML file that contains the Applications Launch Control rules.

6. Click the **Open** button.

The imported rules will be displayed in the list in the **Applications Launch Control rules** window.

Removing Applications Launch Control rules

To remove Applications Launch Control rules:

1. Open the **Applications Launch Control rules** window.
2. In the list, select one or more rules that you want to delete.
3. Click the **Remove Selected** button.
4. Click the **Save** button.

The selected Applications Launch Control rules are deleted.

Configuring a Rule Generator for Applications Launch Control task

To configure the Rule Generator for Applications Launch Control task settings:

1. Open the **Task settings** window of the **Rule Generator for Applications Launch Control** task.
2. Configure the following settings:
   - On the **General** tab:
     - Specify **Prefix for rule names**.
     - Configure the allowing rules usage scope.
   - On the **Actions** tab, specify the actions that must be performed by Kaspersky Embedded Systems Security for Windows.
   - On the **Schedule** and **Advanced** tabs, configure the task start schedule.
   - On the **Run as** tab, configure Task start settings with account permissions.
   - On the **Exclusions** tab, configure exclusions for the Rule Generator for Applications Launch Control task.

a. Select the **Use list of exclusions** check box.

If the check box is selected, the task does not generate Applications Launch Control allow rules for the specified files and executable files from the specified folders.

If the check box is cleared, the task generates Applications Launch Control allow rules in accordance with the settings on the **General** tab.

By default, the check box is selected, and the exclusions list is empty.

b. In the field below, enter the file or folder name. The task will not generate Applications Launch Control allow rules for the specified file or executable files from the specified folder.

c. Click the **Add** button.

The exclusion will be displayed in the list.

d. If necessary, complete steps b and c to add further exclusions.

3. Click the **OK** button in the **Task settings** window.

Kaspersky Embedded Systems Security for Windows immediately applies the new settings to the running task. Information about the date and time when the settings were modified, and the values of task settings before and after modification.

Restricting the task usage scope

To restrict the scope of the Rule Generator for Applications Launch Control task:

1. Open the **Task settings** window of the **Rule Generator for Applications Launch Control** task.
2. On the **General** tab, select how to create allow rules:
   - **Create allowing rules based on running applications**.
   - **Create allowing rules for applications from the folders**.
3. Click the **OK** button in the **Task settings** window.

The specified settings are saved.

Actions to perform during automatic rule generation

To configure the actions of Kaspersky Embedded Systems Security for Windows during the running and upon the completion of the Rule Generator for Applications Launch Control task:

1. Open the **Task settings** window of the **Rule Generator for Applications Launch Control** task.
2. Open the **Options** tab.

3. In the **While generating allowing rules** block, configure the following settings:

   - Use digital certificate
   - Use digital certificate subject and thumbprint
   - If the certificate is missing, use
     - **SHA256 hash**. The checksum of the file used to generate the rule is set as a criterion for triggering the allowing rule for Applications Launch Control. The application will allow start of programs launched using files with the specified checksum.
     - **path to file**. The path to the file used to generate the rule is set as a criterion for triggering the allowing rule for Applications Launch Control. The application will now allow start of programs launched using files located in the folders specified in the **Create allowing rules for applications from the folders** table in the **Settings** section.
   - Use SHA256 hash
   - Generate rules for user or group of users.

4. In the **After task completes** block, configure the following settings:

   - Add allowing rules to the list of Applications Launch Control rules.
   - Principle of adding.
   - **Export allowing rules to file**.
   - Add protected device details to file name.

5. Click the **OK** button in the **Task settings** window.

The specified settings are saved.

Actions to perform upon completion of automatic rule generation

To configure the actions to be taken by Kaspersky Embedded Systems Security for Windows after the Rule Generator for Applications Launch Control task is finished:

1. Open the Task settings window of the **Rule Generator for Applications Launch Control** task.
2. Open the **Options** tab.
3. In the **After task completes** block, configure the following settings:

   - Add allowing rules to the list of Applications Launch Control rules.
   - Principle of adding.
   - **Export allowing rules to file**.
   - Add protected device details to file name.

4. Click the **OK** button in the **Task settings** window.

The specified settings are saved.

Managing Applications Launch Control via the Web Plug-in

To configure Applications Launch Control tasks via the Web Plug-in:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.
2. Click the policy name you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.
4. Select the **Local activity control** section.
5. Click the **Settings** button in the **Applications Launch Control** subsection.
6. Configure the settings described in the table below.

Applications Launch Control task settings

Setting	Description
Task mode.	In this drop-down list, you can select the Applications Launch Control task's mode: • **Active**. Kaspersky Embedded Systems Security for Windows uses the specified rules to control the launch of any application. • **Statistics only**. Kaspersky Embedded Systems Security for Windows does not use Applications Launch Control rules. It only records information about the start of applications in the task log. All applications are allowed to start. You can use this mode to generate a list of Applications Launch Control rules based on the information about denied application launches recorded in the task log. By default, the Applications Launch Control task runs in **Statistics only** mode.
Repeat action taken for the first file launch on all the subsequent launches for this file	The check box enables or disables launch control for the second and subsequent attempts to start applications based on the event information stored in the cache. If the check box is selected, Kaspersky Embedded Systems Security for Windows allows or denies subsequent launches of an application based on the task's conclusion regarding the first launch of the application. For example, if the first application launch was allowed by the rules, information about this decision will be stored in the cache, and the second and all subsequent launches will also be allowed without rechecking. If the check box is cleared, Kaspersky Embedded Systems Security for Windows analyzes an application every time a launch is attempted. By default, the check box is cleared.
Deny the command interpreters launch with no command to execute	If the check box is selected, Kaspersky Embedded Systems Security for Windows denies the launch of command line interpreters even if launching interpreters is allowed. A command line interpreter can only be launched with no command if both of the following conditions are met: • Launch of the command line interpreter is allowed. • The command to be executed is allowed.

	If the check box is cleared, Kaspersky Embedded Systems Security for Windows only considers allowing rules when launching a command line interpreter. The launch is denied if no allowing rule applies or the executable process is not trusted by KSN. If an allowing rule applies or the process is trusted by KSN, a command line interpreter can be launched with or without a command to execute. Kaspersky Embedded Systems Security for Windows recognizes the following command line interpreters: • cmd.exe • powershell.exe • python.exe • perl.exe By default, the check box is cleared.
Apply rules to executable files	The check box either enables or disables launch control of executable files. If this check box is selected, Kaspersky Embedded Systems Security for Windows allows or blocks start of executable files using the specified rules whose settings specify **Executable files** as the scope. If the check box is cleared, Kaspersky Embedded Systems Security for Windows does not control start of executable files using the specified rules. Startup of executable files is allowed. The check box is selected by default.
Monitor loading of DLL modules	The check box either enables or disables control of loading of DLL modules. If this check box is selected, Kaspersky Embedded Systems Security for Windows allows or blocks loading of DLL modules using the specified rules whose settings specify **Executable files** as the scope. If this check box is cleared, Kaspersky Embedded Systems Security for Windows does not control loading of DLL modules using the specified rules. Loading of DLL modules is allowed. The check box is active if the **Apply rules to executable files** check box is selected. The check box is selected by default.
Apply rules to scripts and MSI packages	The check box either enables or disables launch of scripts and MSI packages. If this check box is selected, Kaspersky Embedded Systems Security for Windows allows or blocks start of scripts and MSI packages using the specified rules whose settings specify **Scripts and MSI packages** as the scope. If the check box is cleared, Kaspersky Embedded Systems Security for Windows does not control start of scripts and MSI packages using specified rules. Start of scripts and MSI packages is allowed. The check box is selected by default.
Deny applications untrusted by KSN	The check box either enables or disables Applications Launch Control according to application reputation data in KSN. If this check box is selected, Kaspersky Embedded Systems Security for Windows blocks any application from running if it is not trusted in KSN. Applications Launch Control allowing rules that apply to applications not trusted in KSN will not be triggered. Selecting the check box provides additional protection from malware.

	If the check box is cleared, Kaspersky Embedded Systems Security for Windows does not consider the reputation of applications not trusted in KSN and allows or blocks start in accordance with the rules that apply to such applications. By default, the check box is cleared.
Allow applications trusted by KSN	The check box either enables or disables Applications Launch Control according to application reputation data in KSN. If this check box is selected, Kaspersky Embedded Systems Security for Windows allows applications to run if they are trusted in KSN. Denying application launch control rules that apply to KSN-trusted applications have higher priority: if an application is trusted by KSN services, the application launch will be blocked. If the check box is cleared, Kaspersky Embedded Systems Security for Windows does not consider the reputation of KSN-trusted applications and allows or denies launch in accordance with rules that apply to such applications. By default, the check box is cleared.
Users and / or user groups allowed to run applications trusted by KSN	If the **Allow applications trusted by KSN** check box is selected, here you can specify users and user groups allowed to start applications that are trusted by KSN. By default, the following users are specified: **Everyone** and **NT AUTHORITY\SYSTEM**.
Rules	Configure allowing or denying rules for the Application Launch Control task.
Software Distribution Control	You can add trusted distribution packages.
Task management	You can configure settings to start the task on a schedule.

Device Control

This section contains information about the Device Control task and how to configure it.

About Device Control task

Kaspersky Embedded Systems Security for Windows controls the registration and usage of external and built-in devices and CD/DVD drives to protect the computer against security threats that may arise when these devices share files.

Kaspersky Embedded Systems Security for Windows controls the following devices connections:

- Controlled by default:
  - Removable USB drives, including UAS devices
  - CD/DVD ROM drives
  - USB floppy disk readers
  - USB network adapters
  - MTP mobile devices connected via USB
- Control is disabled by default and needs to be enabled individually:
  - Bluetooth devices connected via USB adapters

    Kaspersky Embedded Systems Security for Windows can monitor Bluetooth devices connected via USB adapters on nodes running Windows 7 SP1 / Server 2008 R2 SP1 or later
  - USB keyboards
  - USB mice
  - SD card readers connected via USB or the PCI bus.

    Kaspersky Embedded Systems Security for Windows does not control SD card readers connected via other interfaces.

The application notifies the user about all devices on the controlled list with an appropriate event in the event and task logs. The event details include device type and connection path.

You can create *Device Control allow rules* (Device Control rules) for devices that you want to allow to connect to the protected device.

The Device Control task monitors attempts by devices on the controlled list to connect to the protected device and blocks the connection if they do not fall within the scope of Device Control rules. After the connection is blocked, the device becomes unavailable.

Kaspersky Embedded Systems Security for Windows identifies devices that are registered in the system, by using the Device Instance Path value. Device Instance Path is a default feature uniquely specified for each external device. The Device Instance Path value is specified for each device in its Windows properties and is determined by Kaspersky Embedded Systems Security for Windows automatically when Device Control rules are generated.

The application assigns one of the following statuses to each connected device on the controlled list:

- *Trusted*. A device that is allowed to connect to the protected device. The device instance path is included in the scope of the Device Control rule.
- *Untrusted*. A device that is blocked from connecting to the protected device. The device instance path is not included in the scope of the Device Control rule.

The Device Control task can operate in two modes:

- **Active**. By default, Kaspersky Embedded Systems Security for Windows blocks all devices on the controlled list, except for trusted ones.

  If an external device you consider to be untrusted is connected to the protected device before the Device Control task starts in *Active* mode, the device will not be blocked by the application. We recommend that you disconnect the untrusted device manually or restart the protected device. Otherwise, the Default Deny principle will not apply to the device.

- **Statistics only**. Kaspersky Embedded Systems Security for Windows does not block controlled devices from connecting. It only adds information about the connection and registration of devices on the protected device, and about the Device Control allow rules triggered by the connected devices, to the task log. This mode is set by default.

About Device Control rules

Kaspersky Embedded Systems Security for Windows does not apply allowing rules for MTP-connected mobile devices.

The rules are generated uniquely for each device that is currently connected or has ever been connected to a protected device if the information about this device is stored in the system registry.

The maximum number of the Device Control rules supported by Kaspersky Embedded Systems Security for Windows is 3072.

Device Control rules are described below.

Rule type

Rule type is always *allowing*. In active mode, the Device Control task blocks access to all controlled device types unless they fall within the scope of at least one Device Control rule.

Triggering criterion and rule usage scope

Device Control rules identify connected devices by *Device instance path* value. The device instance path is a unique ID that the system assigns to a controlled device when it connects to the protected device.

Kaspersky Embedded Systems Security for Windows controls connection of external CD/DVD drives regardless of the bus used for connection. When mounting such device via USB, operating system registers two path values to the device instance: for the external device and for CD/DVD drive (for example, IDE or SCSI). To connect such devices correctly, allowing rules for each path value to the instance must be set.

Kaspersky Embedded Systems Security for Windows automatically defines the device instance path and parses the value obtained into the following elements:

- Device manufacturer (VID)
- Device controller type (PID)
- Device serial number

You cannot set the device instance path manually. Allowing rule triggering criteria define the rule usage scope. By default, the usage scope of a newly created allowing rule includes the one initial device whose properties Kaspersky Embedded Systems Security for Windows used to generate the rule. You can configure the new rule by using a mask to expand the rule application scope.

Initial device values

Device properties that Kaspersky Embedded Systems Security for Windows used for allowing rule generation and that are displayed in Windows Device Manager for each device connected.

Initial device values contain the following information:

- **Device instance path**. Based on this property, Kaspersky Embedded Systems Security for Windows defines rule triggering criteria and fills the following fields: **Manufacturer (VID)**, **Controller type (PID)**, and **Serial number** in the **Rule usage scope** block of the **Rule properties** window.
- **Friendly name**. Device clear name that is set in the device properties by its manufacturer.

Kaspersky Embedded Systems Security for Windows automatically defines initial device values when the rule is generating. Later on you can use these values to recognize the device that was used as a base for the rule generating. Initial device values are not available for editing.

User and group access permissions

By default, when a rule is created, *Everyone (rw)* group is displayed in **Access rights for user or user group** field, which means full access for all users. You can configure access rights to the device described in a rule for one or several users and groups.

Description

You can add further information for each created Device Control rule in the **Description** field, such as the connected device name or owner. The description is displayed in the corresponding field, in the **Device Control rules** window.

The rule ignores the initial device description and values—these only serve the user's reading comfort.

Default Device Control task settings

By default, the Device Control task has the settings described in the table below. You can change the values of these settings.

Default Device Control task settings

Setting	Default value	Description
Task mode.	Statistics only	Kaspersky Embedded Systems Security for Windows does not block controlled external devices from connecting to the protected device. It only adds information about the connection and registration of external devices on the protected device, and about the Device Control allow rules they trigger, to the task log.
Allow using all external devices when the Device Control task is not running	Not applied	If Device Control is running in *Active* mode, regardless of the status of the Device Control task, Kaspersky Embedded Systems Security for Windows blocks external devices from connecting to the protected device unless they fall within the scope of Device Control allow rules.
Block Bluetooth devices.	Not applied	Kaspersky Embedded Systems Security for Windows does not block Bluetooth devices from connecting to the protected device in any Device Control mode. Neither is information about their connections recorded in the Device Control task log.
Block USB keyboards	Not applied	Kaspersky Embedded Systems Security for Windows does not block USB keyboards from connecting to the protected device in any Device Control mode. Neither is information about their connections recorded in the Device Control task log.
Block USB mouses.	Not applied	Kaspersky Embedded Systems Security for Windows does not block USB mice from connecting to the protected device in any Device Control mode. Neither is information about their connections recorded in the Device Control task log.
Block SD card readers connected via USB or PCI bus	Not applied	Kaspersky Embedded Systems Security for Windows does not block access to internal or external USB SD card readers or removable disks connected to internal PCI SD card readers in any Device Control mode.
Task start schedule	First run is not scheduled.	The Device Control task does not start automatically at the start of Kaspersky Embedded Systems Security for Windows. You can configure the task start schedule.

Managing Device Control via the Administration Plug-in

In this section, learn how to configure the Device Control task via the Administration Plug-in.

Configuring Device Control task settings

To configure the Device Control task via the Kaspersky Security Center policy:

1. Go to the Device Control settings in the policy that you want to configure.

   a. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node.

   b. Select the administration group for which you want to configure the task.

   c. Select the **Policies** tab.

   d. Double-click the policy name you want to configure.

   e. In the **Properties: <Policy name>** window that opens, select the **Local activity control** section.

   f. Under **Device Control**, click **Settings**.
   The **Device Control** window opens.

2. On the **General** tab, configure the following task settings:

   - In the **Task mode** block, select one of the following task modes:
     - **Active**.
     - **Statistics only**.
   - Select or clear the **Allow the use of all external devices if the Device Control task is not running** check box.
   - Select or clear the **Block Bluetooth devices** check box.
   - Select or clear the **Block USB keyboards** check box.
   - Select or clear the **Block USB mouses** check box.
   - Select or clear the **Block SD card readers connected via USB or PCI bus** check box.

This check box enables or disables blocking of the following from connecting to the protected device.

- External and internal USB SD card readers
- Removable drives connected to internal PCI SD card readers

If the check box is selected and Device Control is running in *Active* mode, Kaspersky Embedded Systems Security for Windows blocks the devices listed above from connecting to the protected device unless the paths to instances of the devices fall within the scope of Device Control allow rules.

If the check box is selected and Device Control is running in *Statistics only* mode, Kaspersky Embedded Systems Security for Windows does not block the devices listed above from connecting to the protected device. It only adds information about their connections to the protected device, and about the Device Control allow rules they trigger, to the task log.

If the check box is cleared, Kaspersky Embedded Systems Security for Windows does not block devices listed above from connecting to the protected device in any Device Control mode. Neither is information about their connections recorded in the Device Control task log.

By default, the check box is cleared.

3. Click the **Rules list** button to edit the list of Device Control rules.
4. If required, configure the task run schedule on the **Task management** tab.
5. Click **OK** in the **Device Control** window.

Kaspersky Embedded Systems Security for Windows immediately applies the new settings to the running task. Information about the date and time when the settings were modified, and the values of task settings before and after modification, are saved in the system audit log.

Using Device Control rules

This section provides instructions on working with device control rules.

Adding Device Control rules

To add Device Control rules:

1. Go to the Device Control settings in the policy that you want to configure.

a. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node.

b. Select the administration group for which you want to configure the task.

c. Select the **Policies** tab.

d. Double-click the policy name you want to configure.

e. In the **Properties: <Policy name>** window that opens, select the **Local activity control** section.

f. Under **Device Control**, click **Settings**.
The **Device Control** window opens.

2. On the **General** tab, click **Rules list**.
The **Device Control rules** window opens.

3. Add Device Control rules in one of the following ways:

- Use data on currently connected devices

  a. In the **Add** button context menu, select **Generate rules based on connected devices**.
  The **Generate rules based on the system information** window opens.

  b. In the list of detected devices, select those you want to create Device Control rules for.

  c. Click **Create rules for the selected devices**.

- Use system data

  a. In the **Add** button context menu, select **Generate rules based on system data**.
  The **Generate rules based on the system information** window opens.

  b. In the list of detected devices, select those you want to create Device Control rules for.

  c. Click **Create rules for the selected devices**.

- Use the Kaspersky Security Center registry

  a. In the **Add** button context menu, select **Generate rules based on connected devices**.
  The **Generate rules based on the system information** window opens.

  b. Click **Refresh list** to display a list of available devices.

  c. In the list of detected devices, select those you want to create Device Control rules for. In the **Search** field, you can specify a friendly device name to filter the device list and simplify selection.

  d. Click **Create rules for the selected devices**.

- By importing an XML file containing Device Control rules.

  a. In the **Add** button context menu, select **Import rules from XML file**.

  b. Choose how to add Device Control rules from an XML file to those available in the policy:

  - **Merge with existing rules**, if you want to add the imported rules to the list of existing rules. Rules with identical settings are not duplicated. If at least one rule setting is unique, the rule is added.
  - **Add to existing rules**, if you want to add the imported rules to the list of existing rules. Rules with identical settings are duplicated.
  - **Replace existing rules**, if you want to replace the existing rules with the imported rules.

  c. In the Windows system window that opens, specify the path to the XML file that was created after the completion of local task or group task for Rule Generator for Device Control.

  d. Click the **Open** button.

- Import a Kaspersky Security Center blocked devices report.

  Before importing a blocked devices report from Kaspersky Security Center, make sure that it contains only data for those devices you want to allow to connect.

  a. In the **Add** button context menu, select **Import data of blocked devices from Kaspersky Security Center report**.

  b. Choose how to add Device Control rules from a report to those available in the policy:

  - **Merge with existing rules**, if you want to add the imported rules to the list of existing rules. Rules with identical settings are not duplicated. If at least one rule setting is unique, the rule is added.
  - **Add to existing rules**, if you want to add the imported rules to the list of existing rules. Rules with identical settings are duplicated.
  - **Replace existing rules**, if you want to replace the existing rules with the imported rules.

  c. In the Windows system window that opens, specify the path to the TXT file to which events from the Kaspersky Security Center report on blocked devices have been exported.

  d. Click the **Open** button.

The new Device Control rules will be displayed in the list in the **Device Control rules** window.

4. Click **Save** in the **Device Control rules** window.
5. Click **OK** in the **Device Control** window.
6. Click **Apply** in the **Properties: <Policy name>** window.

Viewing Device Control rule properties

To view the properties of a Device Control rule:

1. Go to the Device Control settings in the policy.

   a. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node.

   b. Select the administration group for which you want to configure the task.

   c. Select the **Policies** tab.

   d. Double-click the policy name you want to configure.

   e. In the **Properties: <Policy name>** window that opens, select the **Local activity control** section.

   f. Under **Device Control**, click **Settings**.

   The **Device Control** window opens.

2. On the **General** tab, click **Rules list**.

   The **Device Control rules** window opens.

3. Double-click a rule name to display its properties.

   The **Rule properties** window appears.

Properties of Device Control rules

Property	Description
Apply rule	Use this option to enable or disable the rule application.
Manufacturer (VID)	You can specify the device vendor's full VID or use the * character as a mask. The * character is used to identify any manufacturer. If the Use mask check box is selected for the Manufacturer (VID) field, the data from the field with the selected check box is replaced with the * character and is not considered when the rule is applied.
Controller type (PID)	You can specify the controller's full PID or use the * character as a mask. The * character is used to indicate any type of controller. If the Use mask check box is selected for the Controller type (PID) field, the data from the field with the selected check box is replaced with the * character and is not considered when the rule is applied.
Serial number	You can specify the full serial number of the device, or use the * or ? characters as a mask. An * (asterisk) denotes any sequence of characters, including an empty sequence. A ? (question mark) denotes a single character in a sequence. If the Use mask check box is selected for the Serial number field, the data from the field with the selected check box is replaced with the * character and is not considered when the rule is applied.

	If you selected the **Use a mask** option, but do not enter any characters in the **Serial number** field, then save the settings and close the window, the application applies * as a mask for the **Serial number** property and does not consider the field when the rule is applied.
Device instance path	Identifier of the connected device. The application does not use the field for device control.
Friendly name	Device name set by the manufacturer. The application does not use the field for device control.
User or group of users	You can specify a user account or a group of users with access to the external devices described in this rule: • using Active Directory Domain Services • using the list of users and user groups of the Administration Server • by adding manually. The operating system displays all connected external devices. You can access only those external devices that you have access permission for.
Description	If necessary, add additional information about the Device Control rule to this field. For example, specify devices covered by the rule.

Activating and deactivating Device Control rules

You can activate or deactivate Device Control rules without removing them.

To activate or deactivate a Device Control rule:

1. Go to the Device Control settings in the policy.

   a. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node.

   b. Select the administration group for which you want to configure the task.

   c. Select the **Policies** tab.

   d. Double-click the policy name you want to configure.

   e. In the **Properties: <Policy name>** window that opens, select the **Local activity control** section.

   f. Under **Device Control**, click **Settings**.
   The **Device Control** window opens.

2. On the **General** tab, click **Rules list**.
   The **Device Control rules** window opens.

3. Double-click the name of the Device Control rule to display its settings.

4. In the **Rule properties** window that opens, select or clear the **Apply rule** check box.

5. Click the **OK** button.

The rule application status will be saved and displayed in the **Device Control rules** window.

Expanding Device Control rules usage scope

Each automatically generated Device Control rule allows connecting only one external device. You can manually expand the scope of a Device Control rule by setting a device instance path mask in the rule properties.

Using a device instance path mask reduces the total number of allowing device control rules and simplifies rule processing. However, expanding the scope of Device Control rules can compromise control over connected external devices.

To apply a path mask to a device instance in the Device Control rule properties:

1. Go to the Device Control settings in the policy.

   a. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node.

   b. Select the administration group for which you want to configure the task.

   c. Select the **Policies** tab.

   d. Double-click the policy name you want to configure.

   e. In the **Properties: <Policy name>** window that opens, select the **Local activity control** section.

   f. Under **Device Control**, click **Settings**.

   The **Device Control** window opens.

2. On the **General** tab, click **Rules list**.

   The **Device Control rules** window opens.

3. Double-click the name of the Device Control rule to display its settings.

4. In the **Rule properties** window that opens, do the following:

   - Select the **Use mask** check box next to the **Vendor (VID)** field if you want the rule to allow connections from all external devices with that Vendor ID.
   - Select the **Use mask** check box next to the **Controller type (PID)** field if you want the rule to allow connections from all external devices with that controller type.
   - Select the **Use mask** check box next to the **Serial number** field if you want the rule to allow connections from all external devices with that serial number.

   If the **Use mask** check box is selected in at least one of the fields, the data from the fields with the selected check box is replaced with the * character and is not considered when the rule is applied.

5. If necessary, add further rule details in the **User or group of users access rights** field. For example, specify the devices affected by the rule.

6. Click the **OK** button.

The newly configured rule properties will be saved. The rule usage scope will be expanded according to a device instance path mask specified.

Configuring access permissions

To configure access permissions for a device or class of devices described in a Device Control rule:

1. Go to the Device Control settings in the policy.

   a. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node.

   b. Select the administration group for which you want to configure the task.

   c. Select the **Policies** tab.

   d. Double-click the policy name you want to configure.

   e. In the **Properties: <Policy name>** window that opens, select the **Local activity control** section.

   f. Under **Device Control**, click **Settings**.
   The **Device Control** window opens.

2. On the **General** tab, click **Rules list**.
   The **Device Control rules** window opens.

3. Double-click the name of the Device Control rule to display its settings.

4. In the **Rule properties** window that opens, in **Access rights for user or user group**, click **Settings**.

   Access permissions cannot be configured in Device Control rules created for Bluetooth devices, USB keyboards, and USB mice, as well as in all Device Control rules created for computers running Windows XP or Windows Server 2003 operating systems. These rules allow full access by all users by default.

   The **Setting access rights** window opens.

5. Add rules for accessing the device:

   a. Click the **Add** button.

   b. In the **User or user group access rights** window that opens, click **Browse**.

   c. Select or specify a user or group in any of the suggested ways.

   d. In the **Access rights** drop-down list, select a level of access to the device:

   - **Full control**. All operations on the device contents are allowed.
   - **Read**. You can view files and folders, and run files stored on the device.

e. Click the **OK** button.

f. Complete the steps a through e to add the next device access rule.

g. Click **OK** in the **Setting access rights** window.

6. Rules for accessing the device will be displayed in the **Access rights for user or user group** field.

7. Click the **OK** button.

The configured access permissions for a device or a class of devices described in the Device Control rule will be saved.

After applying the modified Kaspersky Security Center policy, access to devices is provided as follows.

- If a user or group has been granted full access in the Device Control rule settings, they can perform any action on files once the device is connected.
- If a user or group has been granted read access in the Device Control rule settings, they can view files and folders, and open files once the device is connected.
- If a user or group has no specific access rules set in the Device Control rule settings, they will be able to see the device in File Explorer after connecting it, but they will not be able to view its contents.
- If a user or group has its access permissions defined across multiple access rules, the most permissive device access rule will be applied.

To control access to SD card readers connected to the PCI bus after applying a Kaspersky Security Center policy, either restart your computer or remove and re-connect the device for the changes to take effect.

Exporting Device Control rules

To export Device Control rules to an XML file from the Device Control settings in a Kaspersky Security Center policy:

1. Go to the Device Control settings in the policy.

   a. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node.

   b. Select the administration group for which you want to configure the task.

   c. Select the **Policies** tab.

   d. Double-click the policy name you want to configure.

   e. In the **Properties: <Policy name>** window that opens, select the **Local activity control** section.

   f. Under **Device Control**, click **Settings**.
   The **Device Control** window opens.

2. On the **General** tab, click **Rules list**.

   The **Device Control rules** window opens.

3. Click the **Export to a file** button.

   The standard Microsoft Windows **Save as** window opens.

4. In the window that opens, specify the XML file you want to export the rules to. If no such file exists, it will be created. If a file with the specified name already exists, its contents will be overwritten.

5. Click the **Save** button.

Device Control rules will be exported to the specified XML file.

Creating rules with the Rule Generator for Device Control local task

A local Rule Generator for Device Control task allows automatically adding Device Control rules for external devices connected to the protected computer to the settings of the local Device Control task and generating an XML file with the Device Control rules. After that, you can import the XML file in the Device Control settings, in the Kaspersky Security Center group policy or in the local Device Control task on any protected computer.

To secure the protected device, we recommend finalizing the list of Device Control rules before running the Device Control task in active mode. For this reason, we recommend collecting data on connections from controlled external devices in Device Control *Statistics Only* mode.

To set up Device Control rules using a local Rule Generator for Device Control task:

1. Open the properties of the policy that manages the device you are planning to connect external devices to.

2. Enable Device Control *Statistics Only* mode.

3. Activate the policy.

4. Connect the controlled external devices you want to create Device Control rules for to the protected computer.

5. Go to the settings of the local Rule Generator for Device Control task.

6. Go to the **Configuration** section.

7. Select a task running mode under **Mode**:

   - **Consider system data about all external devices that have ever been connected**

   - **Consider currently connected external devices only**

8. Under **After task completes**, specify actions for Kaspersky Embedded Systems Security for Windows to perform upon task completion:

   - **Add allowing rules to the list of Device Control rules**.

   - **Principle of adding**.

   - **Export allowing rules to file**.

- Add protected device details to file name.

9. If you have enabled the **Export allowing rules to file** action, specify the path to the XML file the Device Control rules will be saved to.

   a. Click the **Select** button.

   b. An **Open** window opens.

   c. Specify the path where you want to save the XML file containing the Device Control rules.

   d. In the field with the same name, enter the name of the XML file.

   e. Click the **Open** button.

   The full path to the XML file and the file name will be displayed in the **Settings** window.

10. In the **Properties: Rule Generator for Device Control** window, click **OK**.

11. In the list of tasks, select the previously configured Rule Generator for Device Control task.

12. In the context menu of the Rule Generator for Device Control task, select **Run** to start the task.

When the task completes, the automatically generated Device Control rules will be saved in the settings of the local Device Control task and/or to an XML file inside the specified folder.

Generating a Kaspersky Security Center blocked devices report

You can import data on blocked connection attempts from devices from a report generated in Kaspersky Security Center as a result of running the Device Control task, and use this data to create a list of device control allow rules in a custom policy.

To generate a Kaspersky Security Center blocked devices report:

1. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node.

2. Select the administration group you want to run a blocked devices report for.

3. Select the **Policies** tab.

4. Open the policy properties window by double-clicking the name of the policy configured to collect data on blocked devices.

5. In the **Properties: <Policy name>** window that opens, go to **Logs and notifications**.

6. Under **Task logs**, click **Settings**.

   A **Logs settings** window opens on the **Logs** tab.

7. Select *Device Control* from the **Component** drop-down list.

8. Select *Custom* from the **Importance level** drop-down list.

9. In the list of events, select the *Untrusted external device detected and restricted* and *Statistics only: untrusted external device detected* check boxes.

10. Clear the check boxes next to the other events in the list.

11. In the **Log storage** section, make sure that the Device Control log retention period exceeds the planned period of collecting data on blocked devices. The default is 30 days.

    Once the Device Control log retention period expires, logged events will be deleted and will not appear in the report.

12. Activate the policy configured to collect blocked devices data.

13. If required, modify the Device Control mode.

14. When the period allocated for collecting blocked devices data expires, go to the Device Control log storage folder. Its path is specified in the **Logs settings** policy window on the **Logs** tab, in the **Logs folder** field.

15. Open the Device Control TXT log.

16. If required, adjust the list of events in the Device Control log.

Managing Device Control via the Application Console

In this section, learn how to configure the Device Control task via the Application Console.

Configuring Device Control task settings

To configure the Device Control task:

1. In the Application Console, go to the Device Control settings.

   a. In the Application Console tree, expand the **Computer Control** node.

   b. Select the **Device Control** child node.

   c. In the details pane of the **Device Control** child node, click the **Properties** link.
   The **Task settings** window appears.

2. On the **General** tab, configure the following task settings:

   - In the **Task mode** block, select one of the following task modes:

     - **Active**.

     - **Statistics only**.

- Select or clear the **Allow using all external devices when the Device Control task is not running** check box.
- Select or clear the **Block Bluetooth devices** check box.
- Select or clear the **Block USB keyboards** check box.
- Select or clear the **Block USB mouses** check box.
- Select or clear the **Block SD card readers connected via USB or PCI bus** check box.

  This check box enables or disables blocking of the following from connecting to the protected device.
  - External and internal USB SD card readers
  - Removable drives connected to internal PCI SD card readers

  If the check box is selected and Device Control is running in *Active* mode, Kaspersky Embedded Systems Security for Windows blocks the devices listed above from connecting to the protected device unless the paths to instances of the devices fall within the scope of Device Control allow rules.

  If the check box is selected and Device Control is running in *Statistics only* mode, Kaspersky Embedded Systems Security for Windows does not block the devices listed above from connecting to the protected device. It only adds information about their connections to the protected device, and about the Device Control allow rules they trigger, to the task log.

  If the check box is cleared, Kaspersky Embedded Systems Security for Windows does not block devices listed above from connecting to the protected device in any Device Control mode. Neither is information about their connections recorded in the Device Control task log.

  By default, the check box is cleared.

3. If required, on the **Schedule** and **Advanced** tabs, configure the task schedule.
4. In the **Task settings** window, click **OK**.
5. If required, edit the list of device control rules.

Kaspersky Embedded Systems Security for Windows immediately applies the new settings to the running task. Information about the date and time when the settings were modified, and the values of task settings before and after modification, are saved in the system audit log.

Using Device Control rules

This section provides instructions on working with device control rules.

Adding Device Control rules

To add Device Control rules:

1. In the Application Console tree, expand the **Computer Control** node.
2. Select the **Device Control** child node.
3. In the results pane of the **Device Control** node, click the **Device Control rules** link.

The **Device Control rules** window opens.

4. Add Device Control rules in one of the following ways:

- Use data on currently connected devices

  a. In the **Add** button context menu, select **Generate rules based on connected devices**.
  The **Generate rules based on the system information** window opens.

  b. In the list of detected devices, select those you want to create Device Control rules for.

  c. Click the **Add rules for selected devices** button.

- Use system data

  a. In the **Add** button context menu, select **Generate rules based on system data**.
  The **Generate rules based on the system information** window opens.

  b. In the list of detected devices, select those you want to create Device Control rules for.

  c. Click the **Add rules for selected devices** button.

- By importing an XML file containing Device Control rules.

  a. In the **Add** button context menu, select **Import rules from XML file**.

  b. Choose how to add device control rules from an XML file to those available:

  - **Merge with existing rules**, if you want to add the imported rules to the list of existing rules. Rules with identical settings are not duplicated. If at least one rule setting is unique, the rule is added.
  - **Add to existing rules**, if you want to add the imported rules to the list of existing rules. Rules with identical settings are duplicated.
  - **Replace existing rules**, if you want to replace the existing rules with the imported rules.

  c. In the Windows system window that opens, specify the path to the XML file that was created after the completion of Rule Generator for Device Control task or based on Device Control Events.

  d. Click the **Open** button.

The new Device Control rules will be displayed in the list in the **Device Control rules** window.

5. Click **Save** in the **Device Control rules** window.

Exporting Device Control rules

To export device control rules to an XML file:

1. In the Application Console tree, expand the **Computer Control** node.
2. Select the **Device Control** child node.
3. In the results pane of the **Device Control** node, click the **Device Control rules** link.
   The **Device Control rules** window opens.
4. Click the **Export to a file** button.
   The standard Microsoft Windows **Save as** window opens.
5. In the window that opens, specify the XML file you want to export the rules to. If no such file exists, it will be created. If a file with the specified name already exists, its contents will be overwritten.
6. Click the **Save** button.

Device Control rules will be exported to the specified XML file.

Activating and deactivating Device Control rules

You can activate or deactivate Device Control rules without removing them.

To activate or deactivate a created device control rule:

1. In the Application Console tree, expand the **Computer Control** node.
2. Select the **Device Control** child node.
3. In the results pane of the **Device Control** node, click the **Device Control rules** link.
   The **Device Control rules** window opens.
4. Double-click the name of the Device Control rule to display its settings.
5. In the **Rule properties** window that opens, select or clear the **Apply rule** check box.
6. Click the **OK** button.

The rule application status will be saved and displayed in the **Device Control rules** window.

Expanding Device Control rules usage scope

Each automatically generated Device Control rule allows connecting only one external device. You can manually expand the scope of a Device Control rule by setting a device instance path mask in the rule properties.

Using a device instance path mask reduces the total number of allowing device control rules and simplifies rule processing. However, expanding the scope of Device Control rules can compromise control over connected external devices.

To apply a path mask to a device instance in the Device Control rule properties:

1. In the Application Console tree, expand the **Computer Control** node.

2. Select the **Device Control** child node.

3. In the results pane of the **Device Control** node, click the **Device Control rules** link.

   The **Device Control rules** window opens.

4. In the window that opens, select the rule whose properties you want to apply the device instance path mask to.

5. Open the **Rule properties** window by double clicking on a selected device control rule.

6. In the window that opens, perform the following operations:

   - Select the **Use mask** check box next to the **Manufacturer (VID)** field if you want the selected rule to allow connections for all external devices that fit the specified information about device manufacturer.

   - Select the **Use mask** check boxes next to the **Controller type (PID)** field if you want the selected rule to allow connections for all external devices that fit the specified information about controller type.

   - Select the **Use mask** check box next to the **Serial number** field if you want the selected rule to allow connections for all external devices that match the specified information about the device serial number.

   If the **Use mask** check box is selected in at least one of the fields, the data from the fields with the selected check box is replaced with the * character and is not considered when the rule is applied.

7. If necessary, add further rule details in the **User or group of users access rights** field. For example, specify the devices affected by the rule.

8. Click the **OK** button.

The newly configured rule properties will be saved. The rule usage scope will be expanded according to a device instance path mask specified.

Configuring access permissions

This feature is not available for computers running Windows XP and Windows Server 2003 operating systems. For computers running these operating systems, access permissions for a device can be configured without delimitation for users and/or user groups.

To configure access permissions for a device or class of devices described in a Device Control rule:

1. In the Application Console tree, expand the **Computer Control** node.

2. Select the **Device Control** child node.

3. In the results pane of the **Device Control** node, click the **Device Control rules** link.

   The **Device Control rules** window opens.

4. Double-click the name of the Device Control rule to display its settings.

5. In the **Rule properties** window that opens, in **Access rights for user or user group**, click **Settings**.

Access permissions cannot be configured in Device Control rules created for Bluetooth devices, USB keyboards, and USB mice, as well as in all Device Control rules created for computers running Windows XP or Windows Server 2003 operating systems. These rules allow full access by all users by default.

The **User's management** window opens.

6. Add rules for accessing the device:

   a. Click the **Add** button.

   b. In the **User or user group access rights** window that opens, click **Browse**.

   c. Select or specify a user or group in any of the suggested ways.

   d. In the **Access rights** drop-down list, select a level of access to the device:

      - **Full control**. All operations on the device contents are allowed.
      - **Read**. You can view files and folders, and run files stored on the device.

   e. Click the **OK** button.

   f. Repeat steps a through e to add the next device access rule.

   g. Click **OK** in the **User's management** window.

7. Rules for accessing the device will be displayed in the **Access control for user or group of users** field.

8. Click the **OK** button.

The configured access permissions for a device or a class of devices described in the Device Control rule will be saved.

After applying the modified Kaspersky Security Center policy, access to devices is provided as follows.

- If a user or group has been granted full access in the Device Control rule settings, they can perform any action on files once the device is connected.
- If a user or group has been granted read access in the Device Control rule settings, they can view files and folders, and open files once the device is connected.
- If a user or group has no specific access rules set in the Device Control rule settings, they will be able to see the device in File Explorer after connecting it, but they will not be able to view its contents.
- If a user or group has its access permissions defined across multiple access rules, the most permissive device access rule will be applied.

To control access to SD card readers connected to the PCI bus after applying a Kaspersky Security Center policy, either restart your computer or remove and re-connect the device for the changes to take effect.

Creating rules using the Rule Generator for Device Control task

A local Rule Generator for Device Control task allows automatically adding Device Control rules for external devices connected to the protected computer to the settings of the local Device Control task and generating an XML file with the Device Control rules. After that, you can import the XML file in the Device Control settings, in the Kaspersky Security Center group policy or in the local Device Control task on any protected computer.

To secure the protected device, we recommend finalizing the list of Device Control rules before running the Device Control task in active mode. For this reason, we recommend collecting data on connections from controlled external devices in Device Control *Statistics Only* mode.

To create device control rules via the Rule Generator for Device Control task:

1. Enable Device Control *Statistics Only* mode.
2. Connect the controlled external devices you want to create Device Control rules for to the protected computer.
3. In the Application Console tree, expand the **Automated rule generators** node.
4. Select the **Rule Generator for Device Control** child node.
5. In the results pane of the **Properties** child node, click the **Rule Generator for Device Control** link.

   The **Task settings** window appears.
6. On the **General** tab, under **Task mode**, select a task mode:
   - **Consider system data about all external devices that have ever been connected**
   - **Consider currently connected external devices only**
7. In the **After task completes** section, specify the actions that must be performed by Kaspersky Embedded Systems Security for Windows upon task completion:
   - **Add allowing rules to the list of Device Control rules**.
   - **Principle of adding**.
   - **Export allowing rules to file**.
   - **Add protected device details to file name**.
8. If you have enabled the **Export allowing rules to file** action, specify the path to the XML file the Device Control rules will be saved to.

a. Click the **Select** button.

b. An **Open** window opens.

c. Specify the path where you want to save the XML file containing the Device Control rules.

d. In the field with the same name, enter the name of the XML file.

e. Click the **Open** button.

The full path to the XML file and the file name will be displayed in the **Settings** window.

9. Click the **OK** button in the **Task settings** window.
10. In the results pane of the **Properties** node, click **Run** link to start the task.

Once the task completes, automatically created device control rules will be saved in the Device Control settings and/or an XML file in the specified folder.

Creating a rules XML file from Device Control task events

To secure the protected device, we recommend finalizing the list of Device Control rules before running the Device Control task in active mode. For this reason, we recommend collecting data on connections from controlled external devices in Device Control *Statistics Only* mode.

To create an XML file containing a list of device control rules based on Device Control events:

1. Enable Device Control *Statistics Only* mode.
2. Connect the controlled external devices you want to create Device Control rules for to the protected computer.
3. In the Application Console tree, in the results pane of the **Device Control** node, click **Open task log** link.
4. In the **Logs** window click **Generate rules based on events**.

   An **Open** window opens.
5. Specify the path where you want to save the XML file containing the Device Control rules.
6. In the field with the same name, enter the name of the XML file.
7. Click the **Open** button.

Kaspersky Embedded Systems Security for Windows creates an XML file at the specified path, containing a list of rules based on events registered by the Device Control task. You can use this file to add device control rules in the Device Control settings.

Managing Device Control via the Web Plug-in

In this section, learn how to configure the Device Control task via the Web Plug-in.

Configuring Device Control task settings

To configure the Device Control task via the Kaspersky Security Center policy:

1. Go to the Device Control settings in the policy that you want to configure.

   a. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.

   b. Click the policy name you want to configure.

   c. In the **<Policy name>** window that opens, select the **Application settings** tab.

   d. Select the **Local activity control** section.

   e. Under **Device Control**, click **Settings**.

   The **Device Control** window opens.

2. On the **General** tab, configure the following task settings:

   - Select one of the following task modes:
     - **Active**.
     - **Statistics only**.
   - Select or clear the **Allow the use of all external devices if the Device Control task is not running** check box.
   - Select or clear the **Block Bluetooth devices** check box.
   - Select or clear the **Block USB keyboards** check box.
   - Select or clear the **Block USB mouses** check box.
   - Select or clear the **Block SD card readers connected via USB or PCI bus** check box.

This check box enables or disables blocking of the following from connecting to the protected device.

- External and internal USB SD card readers
- Removable drives connected to internal PCI SD card readers

If the check box is selected and Device Control is running in *Active* mode, Kaspersky Embedded Systems Security for Windows blocks the devices listed above from connecting to the protected device unless the paths to instances of the devices fall within the scope of Device Control allow rules.

If the check box is selected and Device Control is running in *Statistics only* mode, Kaspersky Embedded Systems Security for Windows does not block the devices listed above from connecting to the protected device. It only adds information about their connections to the protected device, and about the Device Control allow rules they trigger, to the task log.

If the check box is cleared, Kaspersky Embedded Systems Security for Windows does not block devices listed above from connecting to the protected device in any Device Control mode. Neither is information about their connections recorded in the Device Control task log.

By default, the check box is cleared.

3. On the **Rules** tab, create a list of device control rules.
4. If required, configure the task run schedule on the **Task management** tab.
5. Click **OK** in the **Device Control** window.

Kaspersky Embedded Systems Security for Windows immediately applies the new settings to the running task. Information about the date and time when the settings were modified, and the values of task settings before and after modification, are saved in the system audit log.

Adding Device Control rules

To add Device Control rules:

1. Go to the Device Control settings in the policy that you want to configure.

   a. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.

   b. Click the policy name you want to configure.

   c. In the **<Policy name>** window that opens, select the **Application settings** tab.

   d. Select the **Local activity control** section.

   e. Under **Device Control**, click **Settings**.

   The **Device Control** window opens.

2. Open the **Rules** tab.
3. Add Device Control rules in one of the following ways:

   - Manually

a. Click the **Add** button.

The **Rule properties** window opens.

b. Enter the rule settings.

c. Click the **OK** button.

- By importing an XML file containing Device Control rules.

a. Click the **Import** button.

b. In the Windows system window that opens, specify the path to the XML file that was created after the completion of Rule Generator for Device Control task.

c. Click the **Open** button.

The imported rules will be added to the list of existing rules. Rules with identical settings are not duplicated. If at least one rule setting is unique, the rule is added.

- Use the Kaspersky Security Center registry

a. Click **From KSC Registry**.

A **Generate rules based on Kaspersky Security Center registry** window opens.

b. In the list of detected devices, select those you want to create Device Control rules for. In the **Search** field, you can specify a **Friendly name** for the device to filter the devices and simplify selection.

c. Click the **OK** button.

- Based on a Kaspersky Security Center blocked devices report

a. Click **From KSC report**.

b. In the Windows system window that opens, specify the path to the TXT file to which events from the Kaspersky Security Center report on blocked devices have been exported.

c. Click the **Open** button.

The imported rules will be added to the list of existing rules. Rules with identical settings are not duplicated. If at least one rule setting is unique, the rule is added.

The device control rules will be displayed on the **Rules** tab.

4. In the **Device Control** window, click **OK**.

Configuring access permissions

To configure access permissions for a device or class of devices described in a Device Control rule:

1. Go to the Device Control settings in the policy that you want to configure.

   a. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.

   b. Click the policy name you want to configure.

   c. In the **<Policy name>** window that opens, select the **Application settings** tab.

   d. Select the **Local activity control** section.

   e. Under **Device Control**, click **Settings**.
   The **Device Control** window opens.

2. Open the **Rules** tab.

3. Select the check box next to the name of the device control rule you want to configure access permissions for.

4. Click the **Edit** button.

5. In the **Rule properties** window that opens, click **Configure access rules** under the **Access rights for user or user group** field.

   Access permissions cannot be configured in Device Control rules created for Bluetooth devices, USB keyboards, and USB mice, as well as in all Device Control rules created for computers running Windows XP or Windows Server 2003 operating systems. These rules allow full access by all users by default.

   The **Setting access rights** window opens.

6. Add rules for accessing the device:

   a. Click the **Add** button.

   b. In the **User or user group access rights** window that opens, click **Configure access rules**.

   c. In the window that opens, select a user or group and click **OK**.

   d. In the **Access rights** drop-down list, select a level of access to the device:

   - **Full control**. All operations on the device contents are allowed.
   - **Read**. You can view files and folders, and run files stored on the device.

   e. Click the **OK** button.

   f. Repeat steps a through e to add the next device access rule.

   g. Click **OK** in the **Setting access rights** window.

7. Rules for accessing the device will be displayed in the **Access rights for user or user group** field.

8. Click the **OK** button.

   The configured access permissions for a device or a class of devices described in the Device Control rule will be saved.

   After applying the modified Kaspersky Security Center policy, access to devices is provided as follows.

- If a user or group has been granted full access in the Device Control rule settings, they can perform any action on files once the device is connected.
- If a user or group has been granted read access in the Device Control rule settings, they can view files and folders, and open files once the device is connected.
- If a user or group has no specific access rules set in the Device Control rule settings, they will be able to see the device in File Explorer after connecting it, but they will not be able to view its contents.
- If a user or group has its access permissions defined across multiple access rules, the most permissive device access rule will be applied.

To control access to SD card readers connected to the PCI bus after applying a Kaspersky Security Center policy, either restart your computer or remove and re-connect the device for the changes to take effect.

Exporting Device Control rules

To export Device Control rules to an XML file from the Device Control settings in a Kaspersky Security Center policy:

1. Go to the Device Control settings in the policy that you want to configure.

   a. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.

   b. Click the policy name you want to configure.

   c. In the **<Policy name>** window that opens, select the **Application settings** tab.

   d. Select the **Local activity control** section.

   e. Under **Device Control**, click **Settings**.

      The **Device Control** window opens.

2. Open the **Rules** tab.

3. Click the **Export** button.

   The standard Microsoft Windows **Save as** window opens.

4. In the window that opens, specify the path to save the XML file that you want to export the device control rules to.

5. Click the **Save** button.

The device control rules will be exported to the DeviceControlRule.xml file located at the specified path.

Creating rules with the Rule Generator for Device Control local task

A local Rule Generator for Device Control task allows automatically adding Device Control rules for external devices connected to the protected computer to the settings of the local Device Control task and generating an XML file with the Device Control rules. After that, you can import the XML file in the Device Control settings, in the Kaspersky Security Center group policy or in the local Device Control task on any protected computer.

To secure the protected device, we recommend finalizing the list of Device Control rules before running the Device Control task in active mode. For this reason, we recommend collecting data on connections from controlled external devices in Device Control *Statistics Only* mode.

To set up Device Control rules using a local Rule Generator for Device Control task:

1. Open the properties of the policy that manages the device you are planning to connect external devices to.
2. Enable Device Control *Statistics Only* mode.
3. Activate the policy.
4. Connect the controlled external devices you want to create Device Control rules for to the protected computer.
5. Go to the settings of the local Rule Generator for Device Control task.

   a. In the main window of the Web Console, select **Devices** → **Managed devices**.

   b. Select the name of the protected device you want to create device control rules for.

   c. In the **<Device name>** window that opens, open the **Tasks** tab.

   d. Select the **Rule Generator for Device Control** task.
   A **Rule Generator for Device Control** window opens.

   e. Open the **Application Settings** tab.

6. Select a task running mode under **Mode**:
   - **Consider system data about all external devices that have ever been connected**
   - **Consider currently connected external devices only**
7. Under **After task completes**, specify actions for Kaspersky Embedded Systems Security for Windows to perform upon task completion:
   - Add allowing rules to the list of Device Control rules.
   - Principle of adding.

- Export allowing rules to file.
- Add protected device details to the file name.

8. If you have enabled the **Export allowing rules to file** action, specify the path to the XML file the Device Control rules will be saved to.

   a. Click the **Select** button.

   b. An **Open** window opens.

   c. Specify the path where you want to save the XML file containing the Device Control rules.

   d. In the field with the same name, enter the name of the XML file.

   e. Click the **Open** button.
   The full path to the XML file and the file name will be displayed in the **Settings** window.

9. In the **Rule Generator for Device Control** window, click **Save**.

10. In the list of tasks, select the check box next to the configured Rule Generator for Device Control task.

11. Click **Run** to start the task.

When the task completes, the automatically generated Device Control rules will be saved in the settings of the local Device Control task and/or to an XML file inside the specified folder.

Generating a Kaspersky Security Center blocked devices report

You can import data on blocked connection attempts from devices from a report generated in Kaspersky Security Center as a result of running the Device Control task, and use this data to create a list of device control allow rules in a custom policy.

To generate a Kaspersky Security Center blocked devices report:

1. Open the task log settings in the policy that manages the protected device.

   a. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.

   b. Click the policy name you want to configure.

   c. In the **<Policy name>** window that opens, select the **Application settings** tab.

   d. Select the **Logs and notifications** section.

   e. Under **Task logs**, click **Settings**.
   A **Task logs** window opens on the **Log storage** tab.

2. Make sure that the Device Control log retention period exceeds the planned period of collecting data on blocked devices. The default is 30 days.

   Once the task log retention period expires, logged events will be deleted and will not appear in the report.

3. Activate the policy configured to collect blocked devices data.

4. If required, modify the Device Control mode.

5. After the period allocated for collecting data on blocked devices expires, create a selection of *untrusted device detected and restricted* and *Statistics only: untrusted device detected* events generated by the Device Control task.

6. Start event selection.

7. Export selection results to a TXT file.

   For details on creating, starting, and exporting a selection of events, refer to the *Kaspersky Security Center Web Console Help*.

8. If required, adjust the list of events in the resulting report file.

Firewall Management

This section contains information about the Firewall Management task and how to configure it.

About the Firewall Management task

If Windows Firewall is turned off during installation of Kaspersky Embedded Systems Security for Windows, the Firewall Management task will not be executed after the installation is complete. If Windows Firewall is enabled during installation, the Firewall Management task is run after installation is complete.

If Windows Firewall is managed by a Kaspersky Security Center group policy, the Firewall Management task cannot be started.

The Firewall Management task does not filter network traffic independently, but it lets you manage the Windows Firewall via the Kaspersky Embedded Systems Security for Windows Console, Administration Plug-in, and Web Plug-in.

The task polls the Windows Firewall regularly. By default, the polling interval is set to one minute and cannot be changed.

While running the Firewall Management task, Kaspersky Embedded Systems Security for Windows performs the actions defined by the mode of interaction with Windows Firewall:

- **Observe the state of Windows Firewall**. The application only monitors the status of Windows Firewall and sends a warning event to Kaspersky Security Center if the Windows Firewall is not started.
- **Control the operation of Windows Firewall**. The application controls the operation of Windows Firewall to the extent determined by the following functions:
  - Maintain the state of Windows Firewall

    This feature enables or disables keeping Windows Firewall in the **Enabled / Disabled** state using the drop-down list.

    If the function is enabled, the application performs the following actions:

    - Polls Windows Firewall at an interval of one minute.
    - Reads the status of Windows Firewall.
    - When the status is set to **Enabled**, enables Windows Firewall if it is disabled.
    - When the status is **Disabled**, disables Windows Firewall when it is enabled.

    This feature cannot be disabled if the **Manage settings and rules of Windows Firewall** feature is disabled.

    By default, the feature is enabled and **Enabled** is selected.

  - Manage settings and rules of Windows Firewall.

This feature enables or disables management of Windows Firewall settings and rules.

If the function is enabled, the application performs the following actions:

- Polls Windows Firewall at an interval of one minute.
- Reads and copies Windows Firewall settings, including firewall rules.
- Sets the values of Windows Firewall settings to match the Firewall Management task settings.
- Creates a list of Kaspersky Security Group firewall rules in the Windows Firewall snap-in. This set contains all firewall rules of the Firewall Management task.

  Later, when polling Windows Firewall, the application does not synchronize the list of Kaspersky Security Group firewall rules with the list of rules of the Firewall Management task. To synchronize the lists of firewall rules, you must restart the Firewall Management task.
- Restricts the ability to edit Windows Firewall settings and rules using third-party tools or directly in the snap-in (wf.msc). If Windows Firewall settings or rules are changed, within one minute the application rolls back the changes to the settings values defined using the Firewall Management task.

If the function is disabled, the application restores the Windows Firewall settings and rules to the values that the application saved after the first poll of Windows Firewall and no longer manages the Windows Firewall settings and rules.

This feature cannot be disabled if the **Maintain the state of Windows Firewall** feature is disabled.

This feature is enabled by default.

About Firewall rules

If the mode of interaction with Windows Firewall is set to **Control the operation of Windows Firewall**, the Firewall Management task filters network traffic through Windows Firewall by using firewall rules.

Firewall rules for applications control network connections for specified applications. The triggering criterion for these rules is based on the path to an executable application file.

Firewall port rules control network connections for specified ports and protocols (TCP / UDP). The triggering criteria for such rules are the port or port range and the type of protocol.

Port rules involve a broader scope than application rules. By allowing network connections based on port rules, you lower the security level of the protected device.

You can manage firewall rules:

- create and delete firewall rules
- change the settings of firewall rules
- enable or disable firewall rules

Firewall rules created by default

During installation, Kaspersky Embedded Systems Security for Windows creates a set of allowing rules to prevent blocking of applications that are installed together with Kaspersky Embedded Systems Security for Windows. See below for details and limitations.

When installed on a device with any supported version of Windows, Kaspersky Embedded Systems Security for Windows creates a set of rules for incoming network connections:

- Allowing rules for the Kaspersky Embedded Systems Security for Windows Console, (kavfsgt.exe), which is located in the application installation folder. Status: enabled. Rule scope: all addresses. Protocols: TCP and UDP, one rule per protocol.
- Two allowing rules for local port 15000, if Kaspersky Security Center Network Agent is installed on the device. State: enabled. Rule scope: all addresses. Protocols: TCP and UDP, one rule per protocol.

When installing on a device with Windows 7 or higher, Kaspersky Embedded Systems Security for Windows creates a set of rules for outgoing network connections:

- Allowing rules for the Kaspersky Embedded Systems Security for Windows Console, (kavfsgt.exe), which is located in the application installation folder. Status: enabled. Rule scope: all addresses. Protocols: TCP and UDP, one rule per protocol.
- Allowing rules for Kaspersky Embedded Systems Security for Windows, (kavfswp.exe), which is located in the application installation folder. State: enabled. Rule scope: all addresses. Protocols: TCP and UDP, one rule per protocol.
- Two allowing rules for local port 13000, if Kaspersky Security Center Network Agent is installed on the device. State: enabled. Rule scope: all addresses. Protocols: TCP and UDP, one rule per protocol.

When uninstalling Kaspersky Embedded Systems Security for Windows, the application deletes all created firewall rules, except for those created by Kaspersky Security Center Network Agent, such as Kaspersky Security Center WDS and Kaspersky Administration Kit. The application also deletes rules for ICMPv4 and ICMPv6 for Windows 7 and later.

When uninstalling Kaspersky Embedded Systems Security for Windows, the application allows all ICMP connections for operating systems earlier than Windows 7.

Default Firewall Management task settings

The Firewall Management task uses the default settings described in the table below. You can change the values of these settings.

Default Firewall Management task settings

Setting	Default value	Description
Mode of interaction between Kaspersky Embedded Systems Security for Windows and Windows Firewall	**Observe the state of Windows Firewall**	The application only monitors the status of Windows Firewall and sends a notification to Kaspersky Security Center if the Windows Firewall is disabled.
Inbound connections	**Block**	You can create and configure incoming firewall rules to block or allow incoming connections.
Outbound connections	**Allow**	You can create and configure outgoing connections firewall rules to block or allow outgoing connections.

Allow ICMP connections	**Disabled**	This setting allows incoming and outgoing network connections via ICMPv4 and ICMPv6, regardless of the task settings for incoming and outgoing connections.
Task start schedule	N/A	The Firewall Management task does not start automatically at the start of Kaspersky Embedded Systems Security for Windows. You can configure the task start schedule.

Configuring the Firewall Management task using the Administration Plug-in

This section provides instructions on configuring general settings of the Firewall Management task and creating and configuring firewall rules using the Administration Plug-in.

Configuring general settings of the Firewall Management task

To configure general settings of the Firewall Management task using the Administration Plug-in:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of protected devices, select the **Policies** tab and open the Properties: <Policy name> window.
   - To configure the settings of a task or application for an individual protected device, select the **Devices** tab and go to local task settings or application settings.
4. In the **Network activity control** section, in the **Firewall Management** section, click the **Settings** button.

   The **Firewall Management** window opens.
5. On the **General** tab, in the **Windows Firewall integration** block, select the mode of interaction between Kaspersky Embedded Systems Security for Windows and Windows Firewall:
   - **Observe the state of Windows Firewall**. If this option is selected, the application only monitors the status of Windows Firewall and sends a warning event to Kaspersky Security Center if Windows Firewall is not started.

     If this option is selected to replace the **Control the operation of Windows Firewall** option, the application restores the internal settings of Windows Firewall the next time the operating system of the protected device is started.
   - **Control the operation of Windows Firewall**. If this option is selected, the application monitors Windows Firewall to the extent determined by the following settings:
     - Maintain the state of Windows Firewall.
     - Manage settings and rules of Windows Firewall.
     - Allow ICMP connections.

6. In the **Inbound connections** block, configure the settings for incoming network connections:

   - Use the **Action for inbound connections** drop-down list to specify the action that Windows Firewall performs for all incoming network connections, unless otherwise defined in the Firewall rules for incoming connections.

   - If necessary, add Firewall rules for incoming connections.

     Firewall rules for incoming connections perform the role of exclusions. For example, if you configure an allowing rule for incoming network connections, and you select **Block** in the **Action for inbound connections** drop-down list, Windows Firewall allows incoming network connections that match the rule criteria.

7. In the **Outbound connections** block, configure the settings for outgoing network connections:

   - Use the **Action for outbound connections** drop-down list to specify the action that Windows Firewall performs for all outgoing network connections, unless otherwise defined in the Firewall rules for outgoing connections.

   - If necessary, add Firewall rules for outgoing connections.

     Firewall rules for outgoing connections perform the role of exclusions. For example, if you configure a blocking rule for outgoing network connections, and select **Allow** in the **Action for outbound connections** drop-down list, Windows Firewall blocks outgoing network connections that match the rule criteria.

8. Click the **OK** button to save the changes.

Kaspersky Embedded Systems Security for Windows applies the new settings to the running task. The date and time when the settings were changed are saved in the system audit log.

Creating and configuring firewall rules

To create and configure firewall rules using the Administration Plug-in:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.

2. Select the administration group for which you want to configure application settings.

3. Perform one of the following actions in the details pane of the selected administration group:

   - To configure application settings for a group of protected devices, select the **Policies** tab and open the **Properties: <Policy name>** window.

   - To configure the settings of a task or application for an individual protected device, select the **Devices** tab and go to local task settings or application settings.

4. In the **Network activity control** section, in the **Firewall Management** section, click the **Settings** button.

   The **Firewall Management** window opens.

5. On the **General** tab, in the **Inbound connections** section, click the **Rules list** button.

   The **Firewall rules for inbound connections** window opens.

6. Create and configure firewall rules for incoming connections.

1. Click the **Add** button on the **Applications** tab.

   The **Firewall rule for application** window opens.

2. Configure the rule settings:

   a. In the **Rule name** field enter the name of the edited rule.

   > The name of the rule, regardless of the case of characters, must not match the reserved names All, ICMPv4, and ICMPv6; it must be unique in the list of all rules for inbound network connections.

   b. In the **Rule action** list, select one of the options:

   - **Allow**. If this option is selected, the application allows incoming network connections for the application.
   - **Block**. If this option is selected, the application blocks incoming network connections for the application.

   c. In the **Application path** field, manually or by using the **Browse** button, specify the path to the executable file of the application for which you are configuring the rule.

   d. In the **Rule action** field, specify network addresses. The application monitors incoming connections from the specified network addresses in accordance with the rule settings.

   > You can only use IPv4 addresses.

   e. Click the **OK** button to save the rule.

3. Click the **Add** button on the **Ports** tab.

   The **Firewall rule for ports** window opens.

4. Configure the rule settings:

   a. In the **Rule name** field enter the name of the edited rule.

   b. In the **Rule action** list, select one of the options:

   - **Allow**. If this option is selected, the application allows incoming network connections for the ports.
   - **Block**. If this option is selected, the application blocks incoming network connections for the ports.

   c. In the **Local ports** block, specify a port or port range.

   d. Select the type of protocol (TCP / UDP) for which the application will control incoming connections.

   e. In the **Rule action** field, specify network addresses. The application monitors incoming connections from the specified network addresses in accordance with the rule settings.

You can only use IPv4 addresses.

f. Click the **OK** button to save the rule.

5. In the **Firewall rules for inbound connections** window, click the **OK** button.

7. On the **General** tab, in the **Outbound connections** block, click on the **Rules list** button.
   The **Firewall rules for outbound connections** window opens.

8. Create and configure firewall rules for outgoing connections.

1. Click the **Add** button on the **Applications** tab.

   The **Firewall rule for application** window opens.

2. Configure the rule settings:

   a. In the **Rule name** field enter the name of the edited rule.

   > The name of the rule, regardless of the case of characters, must not match the reserved names All, ICMPv4, and ICMPv6; it must be unique in the list of all rules for outbound network connections.

   b. In the **Rule action** list, select one of the options:

   - **Allow**. If this option is selected, the application allows outgoing network connections for the application.
   - **Block**. If this option is selected, the application blocks outgoing network connections for the application.

   c. In the **Application path** field, manually or by using the **Browse** button, specify the path to the executable file of the application for which you are configuring the rule.

   d. In the **Rule action** field, specify network addresses. The application monitors outgoing connections to the specified network addresses in accordance with the rule settings.

   > You can only use IPv4 addresses.

   e. Click the **OK** button to save the rule.

3. Click the **Add** button on the **Ports** tab.

   The **Firewall rule for ports** window opens.

4. Configure the rule settings:

   a. In the **Rule name** field enter the name of the edited rule.

   b. In the **Rule action** list, select one of the options:

   - **Allow**. If this option is selected, the application allows outgoing network connections for the ports.
   - **Block**. If this option is selected, the application blocks outgoing network connections for the ports.

   c. In the **Remote ports** block, specify a port or range of ports.

   d. Select the type of protocol (TCP / UDP) for which the application will control outgoing connections.

   e. In the **Rule action** field, specify network addresses. The application monitors outgoing connections to the specified network addresses in accordance with the rule settings.

You can only use IPv4 addresses.

f. Click the **OK** button to save the rule.

5. In the **Firewall rules for outbound connections** window, click the **OK** button.

9. Click the **OK** button in the **Firewall Management** window.

Kaspersky Embedded Systems Security for Windows applies the new settings to the running task. The date and time when the settings were changed are saved in the system audit log.

Enabling and disabling Firewall rules

To enable or disable an existing rule for filtering incoming network traffic, perform the following actions:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of protected devices, select the **Policies** tab and open the **Properties: <Policy name>** window.
   - To configure the settings of a task or application for an individual protected device, select the **Devices** tab and go to local task settings or application settings.
4. In the **Network activity control** section, click the **Settings** button in the **Firewall Management** subsection.
5. Click the **Rules list** button in the window that opens.

   The **Firewall rules for inbound connections** window opens.
6. Depending on the type of rule whose status you want to change, click the **Inbound** or **Outbound** link, and then select the **Applications** or **Ports** tab.
7. In the rule list, select the rule whose status you want to modify and perform one of the following actions:
   - If you want to enable a disabled rule, select the check box to the left of the rule name.

     The selected rule is enabled.
   - If you want to disable an enabled rule, clear the check box to the left of the rule name.

     The selected rule is disabled.
8. Click the **OK** button in the **Firewall rules for inbound connections** window.
9. Click the **OK** button in the **Firewall Management** window.
10. Click the **OK** button in the **Properties: <Policy name>** window.

The specified task settings are saved. The new rule parameters will be sent to Windows Firewall.

Deleting Firewall rules

You can only delete application and port rules. You cannot delete existing group rules.

To delete an existing rule for filtering incoming network traffic, perform the following actions:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of protected devices, select the **Policies** tab and open the **Properties: <Policy name>** window.
   - To configure the settings of a task or application for an individual protected device, select the **Devices** tab and go to local task settings or application settings.
4. In the **Network activity control** section, click the **Settings** button in the **Firewall Management** subsection.
5. Click the **Rules list** button in the window that opens.
   The **Firewall rules for inbound connections** window opens.
6. Depending on the type of rule whose status you want to modify, select the **Applications** or **Ports** tab.
7. In the rule list, select the rule you want to delete.
8. Click the **Delete** button.
   The selected rule is deleted.
9. Click the **OK** button in the **Firewall rules for inbound connections** window.
10. Click the **OK** button in the **Firewall Management** window.
11. Click the **OK** button in the **Properties: <Policy name>** window.

The specified Firewall Management task settings are saved. The new rule parameters will be sent to Windows Firewall.

Configuring the Firewall Management task using the Application Console

This section provides instructions on configuring general settings of the Firewall Management task and creating and configuring firewall rules using the Application Console interface.

Configuring general settings of the Firewall Management task

Some settings of firewall rules for inbound and outbound connections may be unavailable if the Application Console is connected to the local host (on which it is started) and the settings are not supported by the host operating system.

To configure the general settings of the Firewall Management task using the Application Console:

1. In the Application Console tree, expand the **Computer Control** node.
2. Select the **Firewall Management** child node.
3. Click the **Parameters** link in the details pane of the **Firewall Management** node.

   The **Task settings** window appears.
4. On the **General** tab, in the **Windows Firewall integration** block, select the option for interaction between Kaspersky Embedded Systems Security for Windows and Windows Firewall:

   - **Observe the state of Windows Firewall**. If this option is selected, the application only monitors the status of Windows Firewall and sends a warning event to Kaspersky Security Center if Windows Firewall is not started.

     If this option is selected to replace the **Control the operation of Windows Firewall** option, the application restores the internal settings of Windows Firewall the next time the operating system of the protected device is started.

   - **Control the operation of Windows Firewall**. If this option is selected, the application monitors Windows Firewall to the extent determined by the following settings:

     - Maintain the state of Windows Firewall.
     - Manage settings and rules of Windows Firewall.
     - Allow ICMP connections.
5. In the **The program controls the operation of Windows Firewall according to the settings below** block, configure the following settings:

   - Use the **Action for inbound connections** drop-down list to specify the action that Windows Firewall performs for all incoming network connections, unless otherwise defined in the Firewall rules for incoming connections.
   - If necessary, add Firewall rules for incoming connections.

     Firewall rules for incoming connections perform the role of exclusions. For example, if you configure an allowing rule for incoming network connections, and you select **Block** in the **Action for inbound connections** drop-down list, Windows Firewall allows incoming network connections that match the rule criteria.
   - Use the **Action for outbound connections** drop-down list to specify the action that Windows Firewall performs for all outgoing network connections, unless otherwise defined in the Firewall rules for outgoing connections.
   - If necessary, add Firewall rules for outgoing connections.

     Firewall rules for outgoing connections perform the role of exclusions. For example, if you configure a blocking rule for outgoing network connections, and select **Allow** in the **Action for outbound connections** drop-down list, Windows Firewall blocks outgoing network connections that match the rule criteria.

6. Click the **OK** button to save the changes.

Kaspersky Embedded Systems Security for Windows applies the new settings to the running task. The date and time when the settings were changed are saved in the system audit log.

Creating and configuring firewall rules

To create and configure firewall rules using the Application Console:

1. In the Application Console tree, expand the **Computer Control** node.
2. Select the **Firewall Management** child node.
3. Click the **Inbound** link in the details pane of the **Firewall Management** node.

   The **Firewall rules for inbound connections** window opens.
4. Create and configure firewall rules for incoming connections.

1. Click the **Add** button on the **Applications** tab.

   The **Firewall rule for application** window opens.

2. Configure the rule settings:

   a. In the **Rule name** field enter the name of the edited rule.

   > The name of the rule, regardless of the case of characters, must not match the reserved names All, ICMPv4, and ICMPv6; it must be unique in the list of all rules for inbound network connections.

   b. In the **Rule action** list, select one of the options:

   - **Allow**. If this option is selected, the application allows incoming network connections for the application.
   - **Block**. If this option is selected, the application blocks incoming network connections for the application.

   c. In the **Application path** field, manually or by using the **Browse** button, specify the path to the executable file of the application for which you are configuring the rule.

   d. In the **Rule action** field, specify network addresses. The application monitors incoming connections from the specified network addresses in accordance with the rule settings.

   > You can only use IPv4 addresses.

   e. Click the **OK** button to save the rule.

3. Click the **Add** button on the **Ports** tab.

   The **Firewall rule for ports** window opens.

4. Configure the rule settings:

   a. In the **Rule name** field enter the name of the edited rule.

   b. In the **Rule action** list, select one of the options:

   - **Allow**. If this option is selected, the application allows incoming network connections for the ports.
   - **Block**. If this option is selected, the application blocks incoming network connections for the ports.

   c. In the **Local ports** block, specify a port or port range.

   d. Select the type of protocol (TCP / UDP) for which the application will control incoming connections.

   e. In the **Rule action** field, specify network addresses. The application monitors incoming connections from the specified network addresses in accordance with the rule settings.

You can only use IPv4 addresses.

f. Click the **OK** button to save the rule.

5. In the **Firewall rules for inbound connections** window, click the **OK** button.

5. Click the **Outbound connections** link in the details pane of the **Firewall Management** node.
   The **Firewall rules for outbound connections** window opens.

6. Create and configure firewall rules for outgoing connections.

1. Click the **Add** button on the **Applications** tab.

   The **Firewall rule for application** window opens.

2. Configure the rule settings:

   a. In the **Rule name** field enter the name of the edited rule.

   > The name of the rule, regardless of the case of characters, must not match the reserved names All, ICMPv4, and ICMPv6; it must be unique in the list of all rules for outbound network connections.

   b. In the **Rule action** list, select one of the options:

   - **Allow**. If this option is selected, the application allows outgoing network connections for the application.
   - **Block**. If this option is selected, the application blocks outgoing network connections for the application.

   c. In the **Application path** field, manually or by using the **Browse** button, specify the path to the executable file of the application for which you are configuring the rule.

   d. In the **Rule action** field, specify network addresses. The application monitors outgoing connections to the specified network addresses in accordance with the rule settings.

   > You can only use IPv4 addresses.

   e. Click the **OK** button to save the rule.

3. Click the **Add** button on the **Ports** tab.

   The **Firewall rule for ports** window opens.

4. Configure the rule settings:

   a. In the **Rule name** field enter the name of the edited rule.

   b. In the **Rule action** list, select one of the options:

   - **Allow**. If this option is selected, the application allows outgoing network connections for the ports.
   - **Block**. If this option is selected, the application blocks outgoing network connections for the ports.

   c. In the **Remote ports** block, specify a port or range of ports.

   d. Select the type of protocol (TCP / UDP) for which the application will control outgoing connections.

   e. In the **Rule action** field, specify network addresses. The application monitors outgoing connections to the specified network addresses in accordance with the rule settings.

You can only use IPv4 addresses.

f. Click the **OK** button to save the rule.

5. In the **Firewall rules for outbound connections** window, click the **OK** button.

Kaspersky Embedded Systems Security for Windows applies the new settings to the running task. The date and time when the task settings were changed are saved in the system audit log.

Enabling and disabling Firewall rules

To enable or disable an existing rule for filtering incoming network traffic, perform the following actions:

1. In the Application Console tree, expand the **Computer Control** node.
2. Select the **Firewall Management** child node.
3. Click the **Firewall Management** link in the details pane of the **Firewall rules** node.
   The **Firewall rules** window opens.
4. Depending on the type of rule whose status you want to change, click the **Inbound** or **Outbound** link, and then select the **Applications** or **Ports** tab.
5. In the rule list, select the rule whose status you want to modify and perform one of the following actions:
   - If you want to enable a disabled rule, select the check box to the left of the rule name.
     The selected rule is enabled.
   - If you want to disable an enabled rule, clear the check box to the left of the rule name.
     The selected rule is disabled.
6. Click the **Firewall rules** button in the **Save** window.

The specified task settings are saved. The new rule parameters will be sent to Windows Firewall.

Deleting Firewall rules

You can only delete application and port rules. You cannot delete existing group rules.

To delete an existing rule for filtering incoming network traffic, perform the following actions:

1. In the Application Console tree, expand the **Computer Control** node.
2. Select the **Firewall Management** child node.
3. Click the **Firewall Management** link in the details pane of the **Firewall rules** node.
   The **Firewall rules** window opens.

4. Depending on the type of rule whose status you want to modify, select the **Applications** or **Ports** tab.
5. In the rule list, select the rule you want to delete.
6. Click the **Delete** button.

   The selected rule is deleted.
7. Click the **Firewall rules** button in the **Save** window.

The specified task settings are saved. The new rule parameters will be sent to Windows Firewall.

Configuring the Firewall Management task using the Web Plug-in

This section provides instructions on configuring general settings of the Firewall Management task and creating and configuring firewall rules using the Web Plug-in.

Configuring general settings of the Firewall Management task

To configure the general settings of the Firewall Management task using the Web Plug-in:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.
2. Click the policy name you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.
4. Select the **Network activity control** section.
5. Click the **Settings** button in the **Firewall Management** section.

   The **Firewall Management** window opens.
6. On the **General** tab, in the **Windows Firewall integration** block, select the option for interaction between Kaspersky Embedded Systems Security for Windows and Windows Firewall:

   - **Observe the state of Windows Firewall The program only observes the state of Windows Firewall**. If this option is selected, the application only monitors the status of Windows Firewall and sends a warning event to Kaspersky Security Center if Windows Firewall is not started.

     If this option is selected to replace the **Control the operation of Windows Firewall The program controls the operation of Windows Firewall according to the settings below** option, the application restores the internal settings of Windows Firewall the next time the operating system of the protected device is started.

   - **Control the operation of Windows Firewall The program controls the operation of Windows Firewall according to the settings below**. If this option is selected, the application monitors Windows Firewall to the extent determined by the following settings:

     - Maintain the state of Windows Firewall.
     - Manage settings and rules of Windows Firewall.
     - Allow ICMP connections.

7. In the **Inbound connections** block, configure the settings for incoming network connections:

   - Use the **Action for inbound connections** drop-down list to specify the action that Windows Firewall performs for all incoming network connections, unless otherwise defined in the Firewall rules for incoming connections.

   - If necessary, add Firewall rules for incoming connections.

     Firewall rules for incoming connections perform the role of exclusions. For example, if you configure an allowing rule for incoming network connections, and you select **Block** in the **Action for inbound connections** drop-down list, Windows Firewall allows incoming network connections that match the rule criteria.

8. In the **Outbound connections** block, configure the settings for outgoing network connections:

   - Use the **Action for outbound connections** drop-down list to specify the action that Windows Firewall performs for all outgoing network connections, unless otherwise defined in the Firewall rules for outgoing connections.

   - If necessary, add Firewall rules for outgoing connections.

     Firewall rules for outgoing connections perform the role of exclusions. For example, if you configure a blocking rule for outgoing network connections, and select **Allow** in the **Action for outbound connections** drop-down list, Windows Firewall blocks outgoing network connections that match the rule criteria.

9. Click the **OK** button to save the changes.

Kaspersky Embedded Systems Security for Windows applies the new settings to the running task. The date and time when the settings were changed are saved in the system audit log.

Setting	Description
Firewall rules for applications	You can manage application rules. This type of rule allows targeted network connections for specified applications. The triggering criterion for these rules is based on a path to an executable file.
Firewall rules for ports	You can manage port rules. This type of rule allows network connections for specified ports and protocols (TCP / UDP). The triggering criteria for these rules are based on the port number and protocol type.
Task management	You can configure settings to start the task on a schedule.

Creating and configuring firewall rules

To create and configure firewall rules using the Web Plug-in:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.

2. Click the policy name you want to configure.

3. In the **<Policy name>** window that opens, select the **Application settings** tab.

4. Select the **Network activity control** section.

5. Click the **Settings** button in the **Firewall Management** block.

The **Firewall Management** window opens.

6. Create and configure an incoming firewall rule for the application.

   a. Select the **Applications (inbound connections)** tab.

   b. Click the **Add** button.

   c. In the right part of the window, select the **Use the rule** check box to enable the rule.

   d. In the **Rule name** field enter the name of the edited rule.

      The name of the rule, regardless of the case of characters, must not match the reserved names All, ICMPv4, and ICMPv6; it must be unique in the list of all rules for inbound network connections for applications.

   e. In the **Rule action** list, select one of the options:

      - **Allow**. If this option is selected, the application allows incoming network connections for the application.
      - **Block**. If this option is selected, the application blocks incoming network connections for the application.

   f. In the **Application path** field, manually specify the path to the executable file of the application for which you are configuring the rule.

   g. In the **Rule application scope** field, specify network addresses. The application monitors incoming connections from the specified network addresses in accordance with the rule settings.

      You can only use IPv4 addresses.

   h. Click the **OK** button to save the rule.

7. Create and configure a firewall rule for incoming connections for ports.

a. Select the **Ports (inbound connections)** tab.

b. Click the **Add** button.

c. In the right part of the window, select the **Use the rule** check box to enable the rule.

d. In the **Rule name** field enter the name of the edited rule.

> The name of the rule, regardless of the case of characters, must not match the reserved names All, ICMPv4, and ICMPv6; it must be unique in the list of all rules for inbound network connections for ports.

e. In the **Rule action** list, select one of the options:

- **Allow**. If this option is selected, the application allows incoming network connections for the ports.
- **Block**. If this option is selected, the application blocks incoming network connections for the ports.

f. In the **Local ports** block, specify a port or port range.

g. Select the type of protocol (TCP / UDP) for which the application will control incoming connections.

h. In the **Rule application scope** field, specify network addresses. The application monitors incoming connections from the specified network addresses in accordance with the rule settings.

> You can only use IPv4 addresses.

i. Click the **OK** button to save the rule.

8. Create and configure an outgoing firewall rule for the application.

a. Select the **Applications (outbound connections)** tab.

b. Click the **Add** button.

c. In the right part of the window, select the **Use the rule** check box to enable the rule.

d. In the **Rule name** field enter the name of the edited rule.

> The name of the rule, regardless of the case of characters, must not match the reserved names All, ICMPv4, and ICMPv6; it must be unique in the list of all rules for outbound network connections for applications.

e. In the **Rule action** list, select one of the options:

- **Allow**. If this option is selected, the application allows outgoing network connections for the application.
- **Block**. If this option is selected, the application blocks outgoing network connections for the application.

f. In the **Application path** field, manually specify the path to the executable file of the application for which you are configuring the rule.

g. In the **Rule application scope** field, specify network addresses. The application monitors outgoing connections from the specified network addresses in accordance with the rule settings.

> You can only use IPv4 addresses.

h. Click the **OK** button to save the rule.

9. Create and configure an outgoing firewall rule for ports.

a. Select the **Ports (outbound connections)** tab.

b. Click the **Add** button.

c. In the right part of the window, select the **Use the rule** check box to enable the rule.

d. In the **Rule name** field enter the name of the edited rule.

The name of the rule, regardless of the case of characters, must not match the reserved names All, ICMPv4, and ICMPv6; it must be unique in the list of all rules for outbound network connections for ports.

e. In the **Rule action** list, select one of the options:

- **Allow**. If this option is selected, the application allows outgoing network connections for the ports.
- **Block**. If this option is selected, the application blocks outgoing network connections for the ports.

f. In the **Remote ports** block, specify a port or port range.

g. Select the type of protocol (TCP / UDP) for which the application will control incoming connections.

h. In the **Rule application scope** field, specify network addresses. The application monitors outgoing connections to the specified network addresses in accordance with the rule settings.

You can only use IPv4 addresses.

i. Click the **OK** button to save the rule.

10. Click the **OK** button in the **Firewall Management** window.

Kaspersky Embedded Systems Security for Windows applies the new settings to the running task. The date and time when the settings were changed are saved in the system audit log.

Enabling and disabling Firewall rules

To enable or disable an existing rule for filtering incoming network traffic, perform the following actions:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.
2. Click the policy name you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.
4. Select the **Network activity control** section.
5. Click the **Settings** button in the **Firewall Management** subsection.

6. Depending on the type of the rule whose status you want to modify, select the **Firewall rules for applications** or **Firewall rules for ports** tab.
7. In the rule list, select the rule whose status you want to modify and perform one of the following actions:
   - If you want to enable a disabled rule, switch on the toggle button to the left of the rule name.
   - If you want to disable an enabled rule, switch off the toggle button to the left of the rule name.
8. Click the **OK** button.

The specified task settings are saved. The new rule parameters will be sent to Windows Firewall.

Deleting Firewall rules

You can only delete application and port rules. You cannot delete existing group rules.

To delete an existing rule for filtering incoming network traffic, perform the following actions:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.
2. Click the policy name you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.
4. Select the **Network activity control** section.
5. Click the **Settings** button in the **Firewall Management** subsection.
6. Depending on the type of the rule you want to delete, select the **Firewall rules for applications** or **Firewall rules for ports** tab.
7. In the rule list, select the rule you want to delete.
8. Click the **Delete** button.
   The selected rule is deleted.
9. Click the **OK** button.

The specified task settings are saved. The new rule parameters will be sent to Windows Firewall.

File Integrity Monitor

This section contains information about starting and configuring the File Integrity Monitor task.

About the File Integrity Monitor task

The File Integrity Monitor task is designed to track actions performed with the specified files and folders in the monitoring scopes specified in the task settings. You can use the task to detect file changes that may indicate a security breach on the protected device. You can also configure file changes to be tracked during periods in which monitoring is interrupted.

A *monitoring interruption* occurs when the monitoring scope temporarily falls outside the scope of the task, e.g. if the task is stopped or if an external device is not physically present on a protected device. Kaspersky Embedded Systems Security for Windows reports detected file operations in the monitoring scope as soon as an external device is reconnected.

If the tasks stops running in the specified monitoring scope due to a reinstallation of the File Integrity Monitor component, this does not constitute a monitoring interruption. In this case, the File Integrity Monitor task is not run.

Requirements on the environment

To start the File Integrity Monitor task, the following conditions must be satisfied:

- ReFS or NTFS file systems must be used on the protected device.
- The Windows USN Journal must be enabled. The component queries this journal to receive information about file operations.

  If you enable USN Journal after a rule has been created for a volume and the File Integrity Monitor task has been started, the task must be restarted. If not, the rule will not be applied during monitoring.

Excluded monitoring scopes

You can create excluded monitoring scopes. Exclusions are specified for each separate rule and work only for the indicated monitoring scope. You can specify an unlimited number of exclusions for each rule.

Exclusions have higher priority than the monitoring scope and are not monitored by the task, even if an indicated folder or file is in the monitoring scope. If the settings for one of the rules specify a monitoring scope at a lower level than a folder specified in exclusions, the monitoring scope is not considered when the task is run.

To specify exclusions, you can use the same masks that are used to specify monitoring scopes.

About file operations monitoring rules

The File Integrity Monitor task is run based on file operations monitoring rules. You can use rule triggering criteria to configure the conditions that trigger the task, and adjust the importance level for detected file operations events recorded in the task log.

A file operations monitoring rule is specified for each monitoring scope.

You can configure the following rule triggering criteria:

- Trusted users
- File operation markers

Trusted users

By default, the application treats all user actions as potential security breaches. The trusted user list is empty. You can configure the event importance level by creating a list of trusted users in the file operations monitoring rule settings.

Untrusted user is a status assigned to any user not indicated in the trusted user list in the monitoring scope rule settings. If Kaspersky Embedded Systems Security for Windows detects a file operation performed by an untrusted user, the File Integrity Monitor task records a Critical event in the task log.

Trusted user is a status assigned to a user or group of users authorized to perform file operations in the specified monitoring scope. If Kaspersky Embedded Systems Security for Windows detects file operations performed by a trusted user, the File Integrity Monitor task records an Informational event in the task log.

Kaspersky Embedded Systems Security for Windows cannot determine the users that initiate operations during monitoring interruptions. In this case, the user status is determined to be unknown.

Unknown user is a status assigned to a user if Kaspersky Embedded Systems Security for Windows cannot receive information about a user due to a task interruption or a failure of the data synchronization driver or USN Journal. If Kaspersky Embedded Systems Security for Windows detects a file operation performed by an unknown user, the File Integrity Monitor task records a *Warning* event in the task log.

File operation markers

When the File Integrity Monitor task runs, Kaspersky Embedded Systems Security for Windows uses file operation markers to determine that an action has been performed on a file.

A file operation marker is a unique descriptor that can characterize a file operation.

Each file operation can be a single action or a chain of actions with files. Each action of this kind is equated to a file operation marker. If the marker you specify as a rule triggering criterion is detected in a file operation chain, the application logs an event indicating that the given file operation was performed.

The importance level of the logged events does not depend on the selected file operation markers or the number of events.

By default, Kaspersky Embedded Systems Security for Windows considers all available file operation markers. You can select file operation markers manually in the task's rule settings.

Set file operations markers

File operation ID	File operation marker	Supported file

		systems
BASIC_INFO_CHANGE	Attributes or time markers of a file or folder changed	NTFS, ReFS
COMPRESSION_CHANGE	Compression of a file or folder changed	NTFS, ReFS
DATA_EXTEND	Size of file or folder increased	NTFS, ReFS
DATA_OVERWRITE	Data in a file or folder was overwritten	NTFS, ReFS
DATA_TRUNCATION	File or folder truncated	NTFS, ReFS
EA_CHANGE	Extended file or folder attributes changed	Only NTFS
ENCRYPTION_CHANGE	Encryption status of file or folder changed	NTFS, ReFS
FILE_CREATE	File or folder created for the first time	NTFS, ReFS
FILE_DELETE	File or folder permanently deleted using a SHIFT+DEL combination	NTFS, ReFS
HARD_LINK_CHANGE	Hard link created or deleted for file or folder	Only NTFS
INDEXABLE_CHANGE	Index status of file or folder changed	NTFS, ReFS
INTEGRITY_CHANGE	Integrity attribute changed for a named file stream	Only ReFS
NAMED_DATA_EXTEND	Size of a named file stream increased	NTFS, ReFS
NAMED_DATA_OVERWRITE	Named file stream overwritten	NTFS, ReFS
NAMED_DATA_TRUNCATION	Named file stream truncated	NTFS, ReFS
RENAME_NEW_NAME	New name assigned to file or folder	NTFS, ReFS
REPARSE_POINT_CHANGE	New reparse point created or existing reparse point changed for a file or folder	NTFS, ReFS
SECURITY_CHANGE	File or folder access rights changed	NTFS, ReFS
STREAM_CHANGE	New named file stream created or existing named file stream changed	NTFS, ReFS
TRANSACTED_CHANGE	Named file stream changed by TxF transaction	Only ReFS

Default File Integrity Monitor task settings

By default, the File Integrity Monitor task has the settings described in the table below. You can change the values of the settings in the following components:

- The Administration Plug-in
- The Application Console
- The Web Plug-in

Default File Integrity Monitor task settings

Setting	Default value	Description
Monitoring scope	Not defined	Use this option to specify the folders and files for which actions will be monitored. Monitoring events will be generated for the folders and files in the specified monitoring scope.

Trusted users list	Not defined	Use this option to specify users and/or groups of users, whose actions in the specified folders will be treated as safe by the component.
Log information about file operations that appear during the monitor interruption period	Used	This setting is used to enable or disable the logging of file operations performed in the specified monitoring scopes during periods when the task is idle. By default, statistics are collected for untrusted and unknown users and objects.
Block attempts to compromise the USN log	Used	Use this option to enable or disable protection of the USN log.
Detect and block all file operations in the selected area	Disabled	Select or clear the **Detect and block all file operations in the selected area** check box to block all changes for the selected monitoring scope.
Exclude the following folders from control	Not applied	Use this option to check the use of exclusions for folders in which file operations do not need to be monitored. When the File Integrity Monitor task runs, Kaspersky Embedded Systems Security for Windows skips monitoring scopes specified as exclusions.
Checksum calculation	Not applied	Use this option to configure calculation of the file checksum after changes are made in the file.
Set file operations markers	All available file operation markers are considered	Use this option to specify the set of file operation markers. If a file operation performed in a monitoring scope is characterized by one or more specified markers, Kaspersky Embedded Systems Security for Windows generates an audit event.
Task start schedule	First run is not scheduled.	You can configure settings to start the task on a schedule.

Manage File Integrity Monitor via the Administration Plug-in

In this section, learn how to configure the File Integrity Monitor task via the Administration Plug-in.

Configuring the File Integrity Monitor task

To configure the settings of the File Integrity Monitor task using the Administration Plug-in:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of protected devices, select the **Policies** tab and open the Properties: <Policy name> window.

- To configure the settings of a task or application for an individual protected device, select the **Devices** tab and go to local task settings or application settings.

4. In the **System inspection** section, in the **File Integrity Monitor** block, click the **Settings** button.

   The **File Integrity Monitor** window opens.

5. On the **File operations monitoring settings** tab, configure the following settings:

   - Clear or select the **Log information about file operations that appear during the monitoring interruption period** check box.

     The check box enables or disables monitoring of the file operations specified in the File Integrity Monitor task settings when the task is not running for any reason (removal of a hard disk, task stopped by user, software error).

     If the check box is selected, Kaspersky Embedded Systems Security for Windows will record events in all monitoring scopes when the File Integrity Monitor task is not running.

     If the check box is cleared, the application will not log file operations in monitoring scopes when the task is not running.

     The check box is selected by default.

   - Clear or select the **Block attempts to compromise the USN log** check box.

     The check box enables or disables protection of the USN log.

     If the check box is selected, Kaspersky Embedded Systems Security for Windows will block attempts to delete the USN log or to compromise the USN log's content.

     If the check box is cleared, the application will not monitor changes to the USN log.

     The check box is selected by default.

6. Add the file operations monitoring rules that will determine what the task does.

7. On the **Task management** tab, configure the settings for scheduled task start.

8. Click the **OK** button to save the changes.

Kaspersky Embedded Systems Security for Windows applies the new settings to the running task. Information about the date and time of settings modification are saved in the system audit log.

Creating and configuring a file operations monitoring rule

To create and configure a file operations monitoring rule using the Administration Plug-in:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.

2. Select the administration group for which you want to configure application settings.

3. Perform one of the following actions in the details pane of the selected administration group:

   - To configure application settings for a group of protected devices, select the **Policies** tab and open the **Properties: <Policy name>** window.

- To configure the settings of a task or application for an individual protected device, select the **Devices** tab and go to local task settings or application settings.

4. Do one of the following:

   - If you are creating a file operations monitoring rule in a policy, in the **System inspection** section in the **File Integrity Monitor** block, click the **Settings** button.

     The **File Integrity Monitor** window opens on the **File operations monitoring settings** tab.

   - If you are creating a file operations monitor rule for a local task, in the **Properties: File Integrity Monitor** window, go to the **Settings** section.

5. In the **Monitoring scope** block, click the **Add** button.

   The **File operations monitoring rule** window appears.

6. Add a file operations monitoring scope in one of the following ways:

   - If you want to select a folder or drive through the standard Microsoft Windows dialog:

     a. Click the **Browse** button.

        The standard Microsoft Windows **Browse for folder** window appears.

     b. Select the folder whose file operations you want to monitor.

     c. Click the **OK** button.

   - If you want to specify a monitoring scope manually, add a path using a supported mask:

     - <*.ext> — all files with the extension <ext>, regardless of their location
     - <*\name.ext> — all files with name <name> and extension <ext>, regardless of their location
     - <\dir*> — all files in folder <\dir>
     - <\dir*\name.ext> — all files with the name <name> and extension <ext> in folder <\dir> and all of its child folders

   When specifying a monitoring scope manually, be sure that the path is in the following format: <volume letter>:\<mask>. If the volume letter is missing, Kaspersky Embedded Systems Security for Windows will not add the specified monitoring scope.

7. If necessary, specify trusted users:

   a. On the **Trusted users** tab, in the context menu of the **Add** button, select the method for adding trusted users.

      The **User or user group selection** window opens.

   b. Select the users or groups of users for whom file operations are allowed in the selected monitoring scope.

   c. Click the **OK** button.

By default, Kaspersky Embedded Systems Security for Windows treats all users not on the trusted user list as untrusted, and generates Critical events for them. For trusted users, statistics are compiled.

8. On the **File operation markers** tab, if necessary, specify the file operation markers that you want to monitor:

   a. Select the **Detect file operations based on the following markers** option.

   b. In the list of available file operations select the check boxes next to the operations you want to monitor.

By default, Kaspersky Embedded Systems Security for Windows detects all file operation markers. The **Detect file operations based on all recognizable markers** option is selected.

9. If you want the application to block all file operations for the selected scope, select the **Detect and block all file operations in the selected area** check box.

10. If you want the application to calculate the checksum of a file after it has been modified:

    a. Select the **Calculate checksum for the file if possible. The checksum will be available for viewing in the task report** check box.

    b. In the **Checksum type** drop down list, select one of the options:

    - **MD5 hash**
    - **SHA256 hash**.

11. If necessary, add folders or drives to be excluded from the selected file operations monitoring scope:

    a. On the **Exclusions** tab, select the **Exclude the following folders from control** check box.

    b. Click the **Add** button.

    The **Exclusion from the controlled scope** window opens.

    c. Click the **Browse** button.

    The standard Microsoft Windows **Browse for folder** window appears.

    d. Select a folder or drive.

    e. Click the **OK** button.

The specified folder or drive will be displayed in the list of exclusions on the **Exclusions** tab.

You can also add file operations monitoring scope exclusions manually using the same masks that are used to specify file operations monitoring scopes.

12. Click the **File operations monitoring rule** button in the **OK** window.

The configured file operations monitoring rule is displayed in the **File Integrity Monitor** window / **Properties: File Integrity Monitor** in the **Monitoring scope** block.

Export and import of file operations monitoring rules

You can export file operations monitoring rules created manually in the properties of the File Integrity Monitor task to an XML file.

You can import file operations monitoring rules that were previously exported to an XML file into the properties of the File Integrity Monitor task.

To export or import a file operations monitoring rules using the Administration Plug-in:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of protected devices, select the **Policies** tab and open the **Properties: <Policy name>** window.
   - To configure the settings of a task or application for an individual protected device, select the **Devices** tab and go to local task settings or application settings.
4. Do one of the following:
   - If you want to import or export file operations monitoring rules in a policy, in the **System inspection** section, in the **File Integrity Monitor** block, click the **Settings** button.

     The **File Integrity Monitor** window opens on the **File operations monitoring settings** tab.
   - If you want to import or export file operations monitoring rules for a local task, in the **Properties: File Integrity Monitor** window, go to the **Settings** section.
5. Export or import file operations monitoring rules:
   - How to export file operations monitoring rules.

     1. In the **Monitoring scope** block, click the **Export** button.

        The standard Microsoft Windows **Save as** window opens.
     2. Specify the path to save an XML file with the settings of file operations monitoring rules.
     3. Enter the file name in the corresponding field.
     4. Click the **Save** button.

        The application will save an XML file with the settings of the file operations monitoring rules at the specified path.
   - How to import rules for file operations monitoring rules.

1. In the **Monitoring scope** block, click the **Import** button.
2. In the context menu of the **Import** button, select one of the values:
   - **Merge with existing rules**, if you want to add the imported rules to the list of existing rules. Rules with identical settings are not duplicated. If at least one rule setting is unique, the rule is added.
   - **Add to existing rules**, if you want to add the imported rules to the list of existing rules. Rules with identical settings are duplicated.
   - **Replace existing rules**, if you want to replace the existing rules with the imported rules.

   The standard Microsoft Windows **Open** window opens.
3. Specify the path to the XML file with the settings of the file operations monitoring rules.
4. Click the **Open** button.

   In the **File Integrity Monitor** / **Properties: File Integrity Monitor** window, the imported rules will be displayed in the **Monitoring scope** block.

6. Click the **Save** button to save the changes.

Manage File Integrity Monitor via the Application Console

In this section, learn how to configure the File Integrity Monitor task via the Application Console.

Configuring the File Integrity Monitor task

To configure general settings of the File Integrity Monitor task using the Application Console:

1. In the Application Console tree, expand the **System Inspection** node.
2. Select the **File Integrity Monitor** child node.
3. Click the **Properties** link in the results pane of the **File Integrity Monitor** node.

   The **Task settings** window appears.
4. On the **General** tab, configure the following settings:
   a. Clear or select the **Log information about file operations that appear during the monitor interruption period** check box.

The check box enables or disables monitoring of the file operations specified in the File Integrity Monitor task settings when the task is not running for any reason (removal of a hard disk, task stopped by user, software error).

If the check box is selected, Kaspersky Embedded Systems Security for Windows will record events in all monitoring scopes when the File Integrity Monitor task is not running.

If the check box is cleared, the application will not log file operations in monitoring scopes when the task is not running.

The check box is selected by default.

b. Clear or select the **Block attempts to compromise the USN log** check box.

The check box enables or disables protection of the USN log.

If the check box is selected, Kaspersky Embedded Systems Security for Windows will block attempts to delete the USN log or to compromise the USN log's content.

If the check box is cleared, the application will not monitor changes to the USN log.

The check box is selected by default.

5. On the **Schedule** and **Advanced** tabs, configure the task start schedule.

6. Click the **OK** button to save the changes.

Kaspersky Embedded Systems Security for Windows applies the new settings to the running task. Information about the date and time of settings modification are saved in the system audit log.

Creating and configuring a file operations monitoring rule

To create and configure a file operations monitoring rule using the Application Console:

1. In the Application Console tree, expand the **System Inspection** node.

2. Select the **File Integrity Monitor** child node.

3. Click the **File Integrity Monitor** link in the results pane of the **File operations monitoring rules** node.

   The **File operations monitoring rules** window appears.

4. Specify the path for the file operations monitoring scope in one of the following ways:

   - If you want to select a folder or drive through the standard Microsoft Windows dialog:

     a. On the left side of the window, click the **Browse** button.

     The standard Microsoft Windows **Browse for folder** window appears.

     b. Select the folder whose file operations you want to monitor.

     c. Click the **OK** button.

   - If you want to specify a monitoring scope manually, add a path using a supported mask:

     - <*.ext> — all files with the extension <ext>, regardless of their location

- <*\name.ext> — all files with name <name> and extension <ext>, regardless of their location
- <\dir*> — all files in folder <\dir>
- <\dir*\name.ext> — all files with the name <name> and extension <ext> in folder <\dir> and all of its child folders

When specifying a monitoring scope manually, be sure that the path is in the following format: <volume letter>:\<mask>. If the volume letter is missing, Kaspersky Embedded Systems Security for Windows will not add the specified monitoring scope.

5. Click the **Add** button.

   The monitoring scope will be displayed in the list on the left of the **File operations monitoring rules** window.

6. If necessary, specify trusted users:

   a. On the **Trusted users** tab, click the **Add** button.

      The standard Microsoft Windows **Select users or groups** window opens.

   b. Select users or user groups that will be allowed to perform operations on files in the selected monitoring scope.

   c. Click the **OK** button.

By default, Kaspersky Embedded Systems Security for Windows treats all users not on the trusted user list as untrusted, and generates Critical events for them. For trusted users, statistics are compiled.

7. On the **Set file operations markers** tab, if necessary, specify the file operation markers that you want to monitor:

   a. Select the **Detect file operations based on the following markers** option.

   b. In the list of available file operations select the check boxes next to the operations you want to monitor.

By default, Kaspersky Embedded Systems Security for Windows detects all file operation markers. The **Detect file operations based on all recognizable markers** option is selected.

8. If you want the application to block all file operations for the selected monitoring scope, select the **Detect and block all file operations in the selected area** check box.

9. If you want the application to calculate the checksum of a file after it has been modified:

   a. Under **Checksum calculation**, select **Calculate checksum for a file final version, after the file was changed, if possible. The checksum will be available for viewing in the task log**.

   b. In the **Calculate the checksum using the algorithm** drop down list select one of the options:

      - **MD5 hash**
      - **SHA256 hash**.

10. If necessary, add folders or drives to exclude file operations from monitoring:

    a. On the **Set exclusions** tab, select the **Consider excluded monitoring scope** check box.

    b. Click the **Browse** button.

    The standard Microsoft Windows **Browse for folder** window appears.

    c. Select a folder or drive.

    d. Click the **OK** button.

    e. Click the **Add** button.

    The specified folder or drive will be displayed in the list of exclusions.

    > You can also add file operations monitoring scope exclusions manually using the same masks that are used to specify file operations monitoring scopes.

11. Click the **Save** button.

Export and import of file operations monitoring rules

You can export file operations monitoring rules created manually in the properties of the File Integrity Monitor task to an XML file.

You can import file operations monitoring rules that were previously exported to an XML file into the properties of the File Integrity Monitor task.

To export or import file operations monitoring rules using the Application Console:

1. In the Application Console tree, expand the **System Inspection** node.
2. Select the **File Integrity Monitor** child node.
3. Click the **File Integrity Monitor** link in the results pane of the **File operations monitoring rules** node.

   The **File operations monitoring rules** window appears.
4. Export or import file operations monitoring rules:

   - How to export file operations monitoring rules.

1. In the left part of the **File operations monitoring rules** window, click the **Export** button.

   The standard Microsoft Windows **Save as** window opens.

2. Specify the path to save an XML file with the settings of file operations monitoring rules.

3. Enter the file name in the corresponding field.

4. Click the **Save** button.

   The application will save an XML file with the settings of the file operations monitoring rules at the specified path.

- How to import rules for file operations monitoring rules.

  1. In the left part of the **File operations monitoring rules** window, click the **Import** button.

  2. In the context menu of the **Import** button, select one of the values:

     - **Merge with existing rules**, if you want to add the imported rules to the list of existing rules. Rules with identical settings are not duplicated. If at least one rule setting is unique, the rule is added.
     - **Add to existing rules**, if you want to add the imported rules to the list of existing rules. Rules with identical settings are duplicated.
     - **Replace existing rules**, if you want to replace the existing rules with the imported rules.

     The standard Microsoft Windows **Open** window opens.

  3. Specify the path to the XML file with the settings of the registry access monitoring rules.

  4. Click the **Open** button.

     The imported rules will be displayed in the left part of the **File operations monitoring rules** window.

5. Click the **Save** button to save the changes.

Manage File Integrity Monitor via the Web Plug-in

In this section, learn how to configure the File Integrity Monitor task via the Web Plug-in.

Configuring the File Integrity Monitor task

To configure the settings of the File Integrity Monitor task using the Web Plug-in:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.

2. Click the policy name you want to configure.

3. In the **<Policy name>** window that opens, select the **Application settings** tab.
4. Select the **System Inspection** section.
5. In the **File Integrity Monitor** subsection, click the **Settings** button.

   The **File Integrity Monitor** window opens.
6. On the **File operations monitoring settings** tab, configure the following settings:

   a. Clear or select the **Log information about file operations performed during the monitoring interruption period** check box.

   The check box enables or disables monitoring of the file operations specified in the File Integrity Monitor task settings when the task is not running for any reason (removal of a hard disk, task stopped by user, software error).

   If the check box is selected, Kaspersky Embedded Systems Security for Windows will record events in all monitoring scopes when the File Integrity Monitor task is not running.

   If the check box is cleared, the application will not log file operations in monitoring scopes when the task is not running.

   The check box is selected by default.

   b. Clear or select the **Block attempts to compromise the USN log** check box.

   The check box enables or disables protection of the USN log.

   If the check box is selected, Kaspersky Embedded Systems Security for Windows will block attempts to delete the USN log or to compromise the USN log's content.

   If the check box is cleared, the application will not monitor changes to the USN log.

   The check box is selected by default.
7. On the **Task management** tab, configure the task start schedule.
8. Click the **OK** button to save the changes.

Kaspersky Embedded Systems Security for Windows applies the new settings to the running task. Information about the date and time of settings modification are saved in the system audit log.

Creating and configuring a file operations monitoring rule

To create and configure a file operations monitoring rule using the Web Plug-in:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.
2. Click the policy name you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.
4. Select the **System Inspection** section.
5. In the **File Integrity Monitor** subsection, click the **Settings** button.

   The **File Integrity Monitor** window opens on the **File operations monitoring settings** tab.

6. Click the **Add** button.

   The **File operations monitoring rule** window appears.

7. In the **Monitor file operations for the scope**, specify a path using one of the supported masks:

   - <*.ext> — all files with the extension <ext>, regardless of their location
   - <*\name.ext> — all files with name <name> and extension <ext>, regardless of their location
   - <\dir*> — all files in folder <\dir>
   - <\dir*\name.ext> — all files with the name <name> and extension <ext> in folder <\dir> and all of its child folders

   When specifying a monitoring scope manually, be sure that the path is in the following format: <volume letter>:\<mask>. If the volume letter is missing, Kaspersky Embedded Systems Security for Windows will not add the specified monitoring scope.

8. On the **Trusted users** tab, if necessary, specify trusted users in one of the following ways:

   - Using the **Add** button:

     a. Click the **Add** button.

     b. In the window that opens, in the **User name** field, specify the user or group of users in SID format.

     c. Click the **OK** button.

   - Using the **Add from the list of Administration Server** button:

     a. Click the **Add from the list of Administration Server** button.

     b. In the window that opens, select a user or user group from the list.

     c. Click the **OK** button.

   Trusted users are allowed to operate on files from the selected monitoring scope.

   By default, Kaspersky Embedded Systems Security for Windows treats all users not on the trusted user list as untrusted, and generates Critical events for them. For trusted users, statistics are compiled.

9. On the **File operation markers** tab, if necessary, specify the file operation markers that you want to monitor:

   a. Select the **Detect file operations based on the following markers** option.

   b. In the list of available file operations select the check boxes next to the operations you want to monitor.

   By default, Kaspersky Embedded Systems Security for Windows detects all file operation markers. The **Detect file operations based on all recognizable markers** option is selected.

10. If you want the application to block all file operations for the selected monitoring scope, select the **Detect and block all file operations in the selected area** check box.

11. If you want the application to calculate the checksum of a file after it has been modified:

    a. Select the **Calculate checksum for the file if possible. The checksum will be available for viewing in the task report** check box.

    b. In the **Checksum type** drop down list, select one of the options:

    - **SHA256 hash**.
    - **MD5 hash**.

12. If necessary, add folders or drives to exclude file operations from monitoring:

    a. On the **Exclusions** tab, select the **Exclude the following folders from control** check box.

    b. Click the **Add** button.

    c. In the window that opens on the right, in the **Folder name** field, enter the path to the folder or drive that you want to exclude from the file operations monitoring scope.

    d. Click the **OK** button.

    The path to the specified folder or drive will be displayed in the list.

13. Click the **OK** button in the **File operations monitoring rule** window.

    The configured file operations monitoring rule will be displayed in the **File Integrity Monitor** window on the **File operations monitoring settings** tab.

Export and import of file operations monitoring rules

You can export file operations monitoring rules created manually in the properties of the File Integrity Monitor task to an XML file.

You can import file operations monitoring rules that were previously exported to an XML file into the properties of the File Integrity Monitor task.

To export or import file operations monitoring rules using the Web Plug-in:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.
2. Click the policy name you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.
4. Select the **System Inspection** section.
5. In the **File Integrity Monitor** subsection, click the **Settings** button.

   The **File Integrity Monitor** window opens on the **File operations monitoring settings** tab.

6. Export or import file operations monitoring rules:

- How to export file operations monitoring rules.

  Click the **Export** button.

  The application saves the FileIntegrityMonitor.xml file with the settings of the file operation monitoring rules in the C:\Users\<User name>\Downloads folder.

- How to import rules for file operations monitoring rules.

  1. Click the **Import** button.

     The standard Microsoft Windows **Open** window opens.

  2. Specify the path to the XML file with the settings of the file operations monitoring rules.

  3. Click the **Open** button.

     The rules imported via rule list merge will be displayed in the **File Integrity Monitor** window on the **File operations monitoring settings** tab.

     If settings of the file integrity monitor rule from the imported rule list are identical to the settings of already existing rule, this rule will not be added from the imported rule list.

7. Click the **OK** button to save the changes.

AMSI Scanner

This section contains information about the AMSI scanner task and how to configure it.

About the AMSI Scanner task

When the AMSI scanner task is running, Kaspersky Embedded Systems Security for Windows controls the execution of scripts created using Microsoft Windows scripting technologies (Active Scripting) such as VBScript or JScript®. The application can also process PowerShell™ scripts and scripts run in the Microsoft Office applications on operating systems with the Antimalware Scan Interface (AMSI) installed. You can allow or block execution of a script that has been found to be dangerous or probably dangerous. If Kaspersky Embedded Systems Security for Windows identifies a script as potentially dangerous, it blocks or allows execution of the script according to your selected action. If the **Block** action is selected, the application allows script execution only if a script has been found to be safe.

Starting from the Microsoft Windows 10 and Microsoft Windows Server 2016 operating system, Kaspersky Embedded Systems Security for Windows supports the Antimalware Scan Interface (AMSI). AMSI allows applications and services to integrate with any antimalware application installed on a device in order for all the executed scripts to be intercepted and scanned by the antimalware.

You can find more information about AMSI functionality on the Microsoft Windows website.

You can configure the AMSI scanner task settings.

Default AMSI Scanner task settings

The AMSI scanner local system task uses the default settings described in the table below. You can change the values of these settings.

Default AMSI scanner task settings

Setting	Default value	Description
Action to perform on dangerous scripts	**Block**	You can specify the action to be performed on detection of probably dangerous scripts: block or allow their execution.
Heuristic analyzer	The **Medium** security level is applied.	The heuristic analyzer can be enabled or disabled. The analysis level can be configured.
Trusted zone	Used	General list of exclusions that can be used in selected tasks.

Configuring AMSI Scanner task settings via the Administration Plug-in

To configure an AMSI scanner task, do the following:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:

- To configure application settings for a group of protected devices, select the **Policies** tab and open the **Properties: <Policy name>** window.
- To configure the settings of a task or application for an individual protected device, select the **Devices** tab and go to local task settings or application settings.

4. In the **Real-time server protection** section of the **Properties: <Policy name>** window, click **Settings** for **AMSI scanner**.
5. In the **Action to perform on dangerous scripts** section on the **General** tab, do one of the following:
   - To allow execution of probably dangerous scripts, select **Allow**.
   - To block execution of probably dangerous scripts, select **Block**.
6. In the **Heuristic analyzer** section, do one of the following:
   - Clear or select the **Use Heuristic Analyzer** check box.
   - If necessary, adjust the level of analysis using the slider.
7. In the **Trusted Zone** section, select or clear the **Apply Trusted Zone** check box.
8. Click the **OK** button.

The newly configured settings are applied.

Configuring AMSI Scanner task settings via the Application Console

To configure an AMSI scanner task, do the following:

1. In the Application Console tree, expand the **Real-Time Computer Protection** node.
2. Select the **AMSI scanner** child node.
3. Click the **Properties** link in the results pane of the node.
   The **Task settings** window opens on the **General** tab.
4. In the **Action to perform on dangerous scripts** section, do one of the following:
   - To allow execution of probably dangerous scripts, select **Allow**.
   - To block execution of probably dangerous scripts, select **Block**.
5. In the **Heuristic analyzer** section, do one of the following:
   - Clear or select the **Use Heuristic Analyzer** check box.
   - If necessary, adjust the level of analysis using the slider.
6. In the **Trusted Zone** section, select or clear the **Apply Trusted Zone** check box.
7. Click the **OK** button.

The newly configured settings are applied.

Configuring AMSI Scanner task settings via the Web Plug-in

To configure an AMSI scanner task, do the following:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.
2. Click the policy name you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.
4. Select the **Real-time computer protection** section.
5. Click **Settings** in the **AMSI scanner** subsection.
6. In the **Action to perform on dangerous scripts** section on the **General** tab, do one of the following:
   - To allow execution of probably dangerous scripts, select **Allow**.
   - To block execution of probably dangerous scripts, select **Block**.
7. In the **Heuristic analyzer** section, do one of the following:
   - Clear or select the **Use Heuristic Analyzer** check box.
   - If necessary, adjust the level of heuristic analysis.
8. In the **Trusted Zone** section, select or clear the **Apply Trusted Zone** check box.
9. Click the **OK** button.

The newly configured settings are applied.

AMSI Scanner task statistics

While the **AMSI scanner** task is running, you can view information about the number of scripts processed by Kaspersky Embedded Systems Security for Windows from the time when the task was started.

To view the AMSI scanner task statistics, do the following:

1. In the Application Console tree, expand the **Real-Time Computer Protection** node.
2. Select the **AMSI scanner** child node.

Current task statistics are displayed in the results pane of the node in the **Management** and **Statistics** sections.

You can view information about objects processed by Kaspersky Embedded Systems Security for Windows since the task was started (see the table below).

AMSI Scanner task statistics

Field	Description

Scripts blocked	Number of scripts blocked by Kaspersky Embedded Systems Security for Windows.
Dangerous scripts detected	Number of dangerous scripts detected.
Probably dangerous scripts detected	Number of probably dangerous scripts detected.
Processed scripts	Total number of processed scripts.

Registry Access Monitor

This section explains how to start and configure the Registry Access Monitor task.

About the Registry Access Monitor task

The Registry Access Monitor task is designed to track actions performed with the specified registry branches and keys in the monitoring scopes defined in the task settings. The task tracks actions within the operating system installed on the device or within the containers Windows Server 2016 and later defined in the monitoring scope. You can use the task to detect the changes indicating a security breach on the protected device.

To start the Registry Access Monitor task, you must configure at least one monitoring rule.

About the registry access monitoring rules

The **Registry Access Monitor** task is run based on registry access monitoring rules. You can use the rule triggering criteria to configure the conditions triggering the task, and set the importance level for the detected events recorded in the task log.

A registry access monitoring rule is specified for each monitoring scope.

You can configure the following rule triggering criteria:

- **Actions**
- **Controlled values**
- **Trusted users**

Actions

When the Registry Access Monitor task is started, Kaspersky Embedded Systems Security for Windows uses a list of actions to monitor the registry (see the table below).

If an action specified as a rule triggering criterion is detected, the application logs a corresponding event.

The importance level of the logged events does not depend on the selected actions or the number of events.

By default, Kaspersky Embedded Systems Security for Windows considers all actions. You can configure the list of actions manually in the task rule settings.

Actions

Action	Restrictions	Operating system
Create key	• For Windows XP and Windows Server 2003, if you add **Actions** to the list of	Windows XP and

	Create key, and then select the **Block operations according to the rules** mode, the key creation is not blocked in the specified operating systems because of the system restrictions. The key is created with a respective notification sent to the log of events. • If you want to forbid creating a specific key via Registry Editor, create a rule for a parent registry key and make sure to add **Actions** to the list of **Create subkeys**, and then select the **Block operations according to the rules** mode.	later
Delete key	If you want to delete a parent key, make sure to clear both the **Delete subkeys** and **Actions** options on the list of monitored **Delete key** for a configured registry key, as you can only delete the parent key with subkeys.	Windows XP and later
Rename Key	N/A	Windows XP and later
Change key security settings	N/A	Windows Vista and later
Delete values	N/A	Windows XP and later
Set values	If you add **Actions** to the list of **Set values**, define the Default **Value or value mask** in the rule for a key, and then select **Block operations according to the rules** mode, the key is not created, because a new key can only be created with a default value.	Windows XP and later
Create subkeys	N/A	Windows XP and later
Delete subkeys	N/A	Windows XP and later
Rename subkeys	N/A	Windows XP and later
Change subkeys security settings	N/A	Windows Vista and later

Registry values

In addition to registry keys monitoring, you can block or monitor changes for the existing registry values. The following options are available:

- **Set value** - create the new registry values or change the existing registry values.
- **Delete value** - delete the existing registry values.

Renaming and changing the security settings are not applicable for the registry values.

Trusted users

By default, the application treats all user actions as potential security breaches. The trusted user list is empty. You can configure the event importance level by creating a list of trusted users in the system registry monitoring rule settings.

Untrusted user is any user not indicated in the trusted user list in the monitoring scope rule settings. If Kaspersky Embedded Systems Security for Windows detects an action performed by an untrusted user, the Registry Access Monitor task records a Critical event in the task log.

Trusted user is a user or a group of users authorized to perform actions within the specified monitoring scope. If Kaspersky Embedded Systems Security for Windows detects an action performed by a trusted user, the Registry Access Monitor task records an Informational event in the task log.

Default Registry Access Monitor task settings

The default settings for the Registry Access Monitor task are described in the table below. You can change the values of the settings in the following components:

- The Administration Plug-in
- The Application Console
- The Web Plug-in

Default Registry Access Monitor task settings

Setting	Default value	Description
Monitoring scope	Not defined	Use this option to define the parent registry keys and subkeys to monitor. The setting is mandatory. If you do not define the setting, the task fails to start. Monitoring events are generated for the parent registry keys and subkeys in the specified monitoring scope.
Actions	All items of the list of actions are selected	Use this option to configure a list of actions as applicable by selecting and clearing the respective check boxes.
Registry Values	Not defined	Use this option to add, modify, and remove the registry values you want to monitor for the defined monitoring scope.
Trusted users	Not defined	You can specify users and groups of users authorized to perform the defined actions for the specified registry keys.
Task mode.	Statistics only	You can select the task mode to **Block operations according to the rules**, or you can select the **Statistics only** mode to receive the notifications.
Task start schedule	Not defined	You can configure the settings to start the task on schedule.

Managing the Registry Access Monitor via the Administration Plug-in

In this section, learn how to configure the Registry Access Monitor task via the Administration Plug-in.

Configuring the Registry Access Monitor task settings

To configure the settings of the Registry Access Monitor task using the Administration Plug-in:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of protected devices, select the **Policies** tab and open the **Properties: <Policy name>** window.
   - To configure the settings of a task or application for an individual protected device, select the **Devices** tab and go to local task settings or application settings.
4. In the **System inspection** section, in the **Registry Access Monitor** block, click the **Settings** button.
   The **Registry Access Monitor** window appears.
5. On the **Registry Access Monitor settings** tab, in the **Task mode** block, select the required option from the list:
   - **Block operations according to the rules**

     If you select the **Block operations according to the rules** mode, Kaspersky Embedded Systems Security for Windows blocks the **Actions** defined for the monitoring scope.

     By default, the **Statistics only** mode is applied.
   - **Statistics only**.

     If the **Statistics only** mode is selected for the monitoring scope, Kaspersky Embedded Systems Security for Windows compiles the statistics for registry key actions according the configured rules.

     By default, the **Statistics only** mode is applied.
6. Add registry access monitoring rules that will determine what the task does.
7. On the **Task management** tab, configure the task start schedule settings.
8. Click the **OK** button to save the changes.

Kaspersky Embedded Systems Security for Windows applies the new settings to the running task. Information about the date and time of settings modification are saved in the system audit log.

Creating and configuring a registry access monitoring rule

Registry access monitoring rules are applied in the order in which they are listed in the **Registry access monitoring rules** block.

To create and configure a registry access monitoring rule using the Administration Plug-in:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of protected devices, select the **Policies** tab and open the **Properties: <Policy name>** window.
   - To configure the settings of a task or application for an individual protected device, select the **Devices** tab and go to local task settings or application settings.
4. Do one of the following:
   - If you are creating a registry access monitoring rule in a policy, in the **System inspection** section, in the **Registry Access Monitor** block, click the **Settings** button.

     The **Registry Access Monitor** opens on the **Registry Access Monitor settings** tab.
   - If you are creating a registry access monitoring rule for a local task, in the **Properties: Registry Access Monitor** window, go to the **Settings** section.
5. In the **Registry access monitoring rules** block, click the **Add** button.

   The **Registry Access Monitoring rule** window appears.
6. In the **Set rule triggering criteria for the specified scope** field, enter the path using a supported mask.

   You can use `?` and `*` as a mask when entering a path.

   If you enter the path to a root registry key, make sure to specify full path without a mask, such as `HKEY_USERS`. Following is a list of valid root registry keys:

   - `HKEY_LOCAL_MACHINE`
   - `HKLM`
   - `HKEY_CURRENT_USER`
   - `HKCU`
   - `HKEY_USERS`
   - `HKUS`
   - `HKU`
   - `HKEY_CURRENT_CONFIG`
   - `HKEY_CLASSES_ROOT`
   - `HKCR`

Avoid using supported masks for the root keys when creating the rules.
If you specify only a root key, such as HKEY_CURRENT_USER, or a root key with a mask for all child keys, such as HKEY_CURRENT_USER*, a vast number of notifications about addressing the specified child keys is generated, which results in the system performance issues. If you specify a root key, such as HKEY_CURRENT_USER, or a root key with a mask for all child keys, such as HKEY_CURRENT_USER*, and select the **Block operations according to the rules** mode, the system is not able to read or change the keys required for OS functioning and fails to respond.

7. On the **Add** tab, configure the list of actions as needed.

8. Specify the registry values that the rule will monitor:

   a. On the **Registry Values** tab, click the **Add** button.

      The **Registry value rule** window opens.

   b. In the corresponding field, enter a registry value mask.

   c. In the **Controlled operations** block, select which actions taken on the registry value will be monitored by the rule.

   d. Click the **OK** button to save the changes.

9. If necessary, specify trusted users:

   a. On the **Trusted users** tab, in the context menu of the **Add** button, select the method for adding trusted users.

      The **User or user group selection** window opens.

   b. Select a user or user group that is allowed to perform the selected actions.

   c. Click the **OK** button to save the changes.

By default, Kaspersky Embedded Systems Security for Windows treats all users not on the trusted user list as untrusted, and generates Critical events for them. For trusted users, statistics are compiled.

10. In the **Registry Access Monitoring rule** window, click the **OK** button.

The configured registry access monitoring rule is displayed in the **Registry Access Monitor** / **Properties: Registry Access Monitor** window in the **Registry access monitoring rules** block.

Export and import of registry access monitoring rules

You can export registry access monitoring rules created manually in the properties of the Registry Access Monitor task to an XML file.

You can import registry access monitoring rules that were previously exported to an XML file into the properties of the Registry Access Monitor task.

To export or import registry access monitoring rules using the Administration Plug-in:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.

2. Select the administration group for which you want to configure application settings.

3. Perform one of the following actions in the details pane of the selected administration group:

   - To configure application settings for a group of protected devices, select the **Policies** tab and open the **Properties: <Policy name>** window.

   - To configure the settings of a task or application for an individual protected device, select the **Devices** tab and go to local task settings or application settings.

4. Do one of the following:

   - If you want to import or export rules for monitoring registry access in a policy, in the **System inspection** section, in the **Registry Access Monitor** block, click the **Settings** button.

     The **Registry Access Monitor** opens on the **Registry Access Monitor settings** tab.

   - If you want to import or export registry access monitoring rules for a local task, in the **Properties: Registry Access Monitor** window, go to the **Settings** section.

5. Export or import registry access monitoring rules:

   - How to export registry access monitoring rules.

     1. In the **Registry access monitoring rules** block, click the **Export** button.

        The standard Microsoft Windows **Save as** window opens.

     2. Specify the path to save the XML file with the settings of the registry access monitoring rules.

     3. Enter the file name in the corresponding field.

     4. Click the **Save** button.

        The application will save an XML file with the settings of the registry access monitoring rules in the specified path.

   - How to import registry access monitoring rules.

1. In the **Registry access monitoring rules** block, click the **Import** button.
2. In the context menu of the **Import** button, select one of the values:
   - **Merge with existing rules**, if you want to add the imported rules to the list of existing rules.

     If the registry branch name in the imported rule matches the registry branch name of an existing rule, the imported rule will not be added even if the values of the settings for this registry branch differ in the rules.

   - **Add to existing rules**, if you want to add the imported rules to the list of existing rules. Rules with identical settings are duplicated.
   - **Replace existing rules**, if you want to replace the existing rules with the imported rules.

   The standard Microsoft Windows **Open** window opens.
3. Specify the path to the XML file with the settings of the registry access monitoring rules.
4. Click the **Open** button.

   In the **Registry Access Monitor** / **Properties: Registry Access Monitor** window, the imported rules will be displayed in the **Registry access monitoring rules** section.

6. Click the **Save** button to save the changes.

Managing the Registry Access Monitor task via the Application Console

In this section, learn how to configure the Registry Access Monitor task via the Application Console.

Configuring general settings of the Registry Access Monitor task

To configure general settings of the Registry Access Monitor task via the Application Console:

1. In the Application Console tree, expand the **System Inspection** node.
2. Select the **Registry Access Monitor** child node.
3. Click the **Properties** link in the results pane of the **Registry Access Monitor** node.

   The **Task settings** window opens on the **General** tab.
4. In the **Task mode** block, select the required option from the list:
   - Block operations according to the rules

If you select the **Block operations according to the rules** mode, Kaspersky Embedded Systems Security for Windows blocks the **Actions** defined for the monitoring scope.

By default, the **Statistics only** mode is applied.

- Statistics only.

  If the **Statistics only** mode is selected for the monitoring scope, Kaspersky Embedded Systems Security for Windows compiles the statistics for registry key actions according the configured rules.

  By default, the **Statistics only** mode is applied.

5. On the **Schedule** and **Advanced** tabs, configure the task start schedule.
6. Click the **OK** button to save the changes.

Kaspersky Embedded Systems Security for Windows applies the new settings to the running task. Information about the date and time of settings modification are saved in the system audit log.

Creating and configuring a registry access monitoring rule

Registry access monitoring rules are applied in the order in which they are listed in the **Registry access monitoring rules** block.

To create and configure a registry access monitoring rule using the Application Console:

1. In the Application Console tree, expand the **System Inspection** node.
2. Select the **Registry Access Monitor** child node.
3. Click the **Registry Access Monitor** link in the results pane of the **Registry Access Monitoring Rules** node.
   The **Registry Access Monitoring** window appears.
4. In the **Add system registry key to monitor** field, enter the path to the registry key using a supported mask.

   Avoid using supported masks for the root keys, when creating the rules.
   If you specify only a root key, such as HKEY_CURRENT_USER, or a root key with a mask for all child keys, such as HKEY_CURRENT_USER*, a vast number of notifications about addressing the specified child keys is generated, which results in the system performance issues.
   If you specify a root key, such as HKEY_CURRENT_USER, or a root key with a mask for all child keys, such as HKEY_CURRENT_USER*, and select the **Block operations according to the rules** mode, the system is not able to read or change the keys required for OS functioning and fails to respond.

5. Click the **Add** button.
6. On the **Actions** tab for the selected monitoring scope, configure the list of actions as needed.
7. Specify the registry values that the rule will monitor:

   a. On the **Controlled values** tab, click the **Add** button.

The **Registry value rule** window opens.

b. In the corresponding field, enter the registry value or registry value mask.

c. In the **Controlled operations** block, select which actions taken on the registry value will be monitored by the rule.

d. Click the **OK** button to save the changes.

8. If necessary, specify trusted users:

a. On the **Trusted users** tab, click the **Add** button.

b. In the **Select Users or Groups** window, select the users or groups of users authorized to perform the selected actions.

c. Click the **OK** button to save the changes.

By default, Kaspersky Embedded Systems Security for Windows treats all users not on the trusted user list as untrusted, and generates Critical events for them. For trusted users, statistics are compiled.

9. In the **Registry Access Monitoring** window, click the **Save** button.

The configured registry access monitoring rule is displayed in the **Registry Access Monitoring** block of the **Registry access monitoring rules** window.

Export and import of registry access monitoring rules

You can export registry access monitoring rules created manually in the properties of the Registry Access Monitor task to an XML file.

You can import registry access monitoring rules that were previously exported to an XML file into the properties of the Registry Access Monitor task.

To export and import registry access monitoring rules using the Application Console:

1. In the Application Console tree, expand the **System Inspection** node.

2. Select the **Registry Access Monitor** child node.

3. Click the **Registry Access Monitor** link in the results pane of the **Registry Access Monitoring Rules** node.

The **Registry Access Monitoring** window appears.

4. How to export registry access monitoring rules.

1. In the **Registry access monitoring rules** block, click the **Export to file** button to export the registry access monitoring rules.

   The standard Microsoft Windows **Save as** window opens.

2. Specify the path to save the XML file with the settings of the registry access monitoring rules.

3. Enter the file name in the corresponding field.

4. Click the **Save** button.

   The application will save an XML file with the settings of the registry access monitoring rules in the specified path.

5. How to import registry access monitoring rules.

   1. In the **Registry access monitoring rules** block, click the **Import** button.

   2. In the context menu of the **Import** button, select one of the values:

      - **Merge with existing rules**, if you want to add the imported rules to the list of existing rules.

        If the registry branch name in the imported rule matches the registry branch name of an existing rule, the imported rule will not be added even if the values of the settings for this registry branch differ in the rules.

      - **Add to existing rules**, if you want to add the imported rules to the list of existing rules. Rules with identical settings are duplicated.

      - **Replace existing rules**, if you want to replace the existing rules with the imported rules.

      The standard Microsoft Windows **Open** window opens.

   3. Specify the path to the XML file with the settings of the registry access monitoring rules.

   4. Click the **Open** button.

   The imported rules will be displayed in the **Registry Access Monitoring** block of the **Registry access monitoring rules** window.

6. Click the **Save** button to save the changes.

Managing the Registry Access Monitor via the Web Plug-in

In this section, learn how to configure the Registry Access Monitor task via the Web Plug-in.

Configuring the Registry Access Monitor task settings

To configure the Registry Access Monitor task via the Web Plug-in:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.
2. Click the policy name you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.
4. Select the **System Inspection** section.
5. In the **Registry Access Monitor** subsection, click the **Settings** button.

   The **Registry Access Monitor** opens on the **Registry Access Monitor settings** tab.
6. In the **Task mode** block, select the required option from the list:

   - **Block operations according to the rules**

     If you select the **Block operations according to the rules** mode, Kaspersky Embedded Systems Security for Windows blocks the **Actions** defined for the monitoring scope.

     By default, the **Statistics only** mode is applied.

   - **Statistics only**

     If the **Statistics only** mode is selected for the monitoring scope, Kaspersky Embedded Systems Security for Windows compiles the statistics for registry key actions according the configured rules.

     By default, the **Statistics only** mode is applied.
7. Add registry access monitoring rules that will determine what the task does.
8. On the **Task management** tab, configure the task start schedule.
9. Click the **OK** button to save the changes.

Kaspersky Embedded Systems Security for Windows applies the new settings to the running task. Information about the date and time of settings modification are saved in the system audit log.

Creating and configuring a registry access monitoring rule

Registry access monitoring rules are applied in the order in which they are listed in the **Registry access monitoring rules** block.

To create and configure a registry access monitoring rule using the Web Plug-in:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.

2. Click the policy name you want to configure.

3. In the **<Policy name>** window that opens, select the **Application settings** tab.

4. Select the **System Inspection** section.

5. In the **Registry Access Monitor** subsection, click the **Settings** button.

   The **Registry Access Monitor** opens on the **Registry Access Monitor settings** tab.

6. In the **Registry access monitoring rules** block, click the **Add** button.

   The **Registry Access Monitoring rule** window appears.

7. In the **Monitor registry access for a scope** field, enter a path using a supported mask.

   You can use `?` and `*` as a mask when entering a path.

   If you enter the path to a root registry key, make sure to specify full path without a mask, such as `HKEY_USERS`. Following is a list of valid root registry keys:

   - `HKEY_LOCAL_MACHINE`
   - `HKLM`
   - `HKEY_CURRENT_USER`
   - `HKCU`
   - `HKEY_USERS`
   - `HKUS`
   - `HKU`
   - `HKEY_CURRENT_CONFIG`
   - `HKEY_CLASSES_ROOT`
   - `HKCR`

   Avoid using supported masks for the root keys, when creating the rules.
   If you specify only a root key, such as HKEY_CURRENT_USER, or a root key with a mask for all child keys, such as HKEY_CURRENT_USER*, a vast number of notifications about addressing the specified child keys is generated, which results in the system performance issues.
   If you specify a root key, such as HKEY_CURRENT_USER, or a root key with a mask for all child keys, such as HKEY_CURRENT_USER*, and select the **Block operations according to the rules** mode, the system is not able to read or change the keys required for OS functioning and fails to respond.

8. On the **Actions** tab for the selected monitoring scope, configure the list of actions as needed.

9. Specify the registry values that the rule will monitor:

   a. On the **Controlled values** tab, click the **Add** button.

The **Registry value rule** window opens.

b. In the corresponding field, enter a registry value mask.

c. In the **Controlled operations** block, select which actions performed with the registry value will be monitored by the rule.

d. Click the **OK** button to save the changes.

10. If necessary, specify trusted users:

a. On the **Trusted users** tab, click the **Add** button.

b. Enter the **User name** or click **Set SID for the group Everyone**, to define users authorized to perform the selected actions.

c. Click the **OK** button to save the changes.

By default, Kaspersky Embedded Systems Security for Windows treats all users not on the trusted user list as untrusted, and generates Critical events for them. For trusted users, statistics are compiled.

11. In the **Registry Access Monitoring rule** window, click the **OK** button to save the changes.

The configured registry access monitoring rule is displayed in the **Registry Access Monitor** block of the **Registry access monitoring rules** window.

Export and import of registry access monitoring rules

You can export registry access monitoring rules created manually in the properties of the Registry Access Monitor task to an XML file.

You can import registry access monitoring rules that were previously exported to an XML file into the properties of the Registry Access Monitor task.

To export or import registry access monitoring rules using the Web Plug-in:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.
2. Click the policy name you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.
4. Select the **System Inspection** section.
5. In the **Registry Access Monitor** block, click the **Settings** button.

   The **Registry Access Monitor** opens on the **Registry Access Monitor settings** tab.
6. Export or import registry access monitoring rules:

   - How to export registry access monitoring rules.

In the **Registry access monitoring rules** block, click the **Export** button.

The application saves the RegistryMonitor.xml file with the settings of registry access monitoring rules in the C:\Users\<User name>\Downloads folder.

- How to import registry access monitoring rules.

  1. In the **Registry access monitoring rules** block, click the **Import** button.
  2. Click the **Import** button.

     The standard Microsoft Windows **Open** window opens.
  3. Specify the path to the XML file with the settings of the registry access monitoring rules.
  4. Click the **Open** button.

     The rules imported via rule list merge will be displayed in the **Registry Access Monitor** block of the **Registry access monitoring rules** window.

     If the registry branch name in the imported rule matches the registry branch name of an existing rule, the imported rule will not be added even if the values of the settings for this registry branch differ in the rules.

7. Click the **Save** button to save the changes.

Log Inspection

This section contains information about the Log Inspection task and task settings.

About the Log Inspection task

When the Log Inspection task runs, Kaspersky Embedded Systems Security for Windows monitors the integrity of the protected environment based on the results of an inspection of Windows event logs. The application notifies the administrator upon detecting abnormal behavior that may indicate attempted cyberattacks.

Kaspersky Embedded Systems Security for Windows analyzes the Windows event logs and identifies breaches based on the rules specified by the user or by the settings of the heuristic analyzer, which the task uses to inspect logs.

Predefined rules and heuristic analysis

You can use the Log Inspection task to monitor the state of the protected system by applying predefined rules based on existing heuristics. The heuristic analyzer identifies abnormal activity on the protected device, which may be evidence of an attempted attack. Templates to identify abnormal behavior are included in the available rules in the predefined rules settings.

Seven rules are included in the rule list for the Log Inspection task. You can enable or disable any of the rules. You cannot delete existing rules or create new rules.

You can configure the triggering criteria for rules that monitor events for the following operations:

- Password brute-force detection
- Network login detection

You can also configure exclusions in the task settings. The heuristic analyzer is not activated when a login is conducted by a trusted user or from a trusted IP address.

Kaspersky Embedded Systems Security for Windows does not use heuristics to inspect Windows logs if the heuristic analyzer is not used by the task. By default, the heuristic analyzer is enabled.

When the rules are applied, the application records a *Critical event* in the Log Inspection task log.

Custom rules for the Log Inspection task

You can use the rule settings to specify and change the criteria for triggering rules upon detecting the selected events in the specified Windows log. By default, the list of Log Inspection rules has four rules. You can enable and disable these rules, remove rules, and edit rule settings.

You can configure the following rule triggering criteria for each rule:

- List of record identifiers in the Windows Event Log.

  The rule is triggered when a new record is created in the Windows Event Log, if the event properties includes an event identifier specified in the rule. You can also add and remove identifiers for each specified rule.

- Event source.

  For each rule, you can specify a log within the Windows Event Log. The application will search for records with the specified event identifiers only in this log. You can select one of the standard logs (Application, Security, or System), or specify a custom log by entering the name in the source selection field.

  > The application does not verify that the specified log actually exists in the Windows Event Log.

When the rule is triggered, Kaspersky Embedded Systems Security for Windows records a Critical event in the Log Inspection task log.

By default, the Log Inspection task applies custom rules.

> Before starting the Log Inspection task make sure the system audit policy is set up correctly. Refer to the Microsoft article for details.

Default Log Inspection task settings

By default, the Log Inspection task has the settings described in the table below. You can change the values of these settings.

Default Log Inspection task settings

Setting	Default value	Description
Apply custom rules for log inspection	Not applied.	You can enable, disable, add, or modify the custom rules.
Apply predefined rules for log inspection	Applied.	You can enable or disable the heuristic analyzer, which detects abnormal activity on the protected device.
Brute-force attack detection	10 logon failures per 300 seconds.	You can set the number of attempts and time frame used, which will be considered as triggers by the heuristic analyzer.
Network logon	12:00:00 AM.	You can indicate the start and end of the time interval during which Kaspersky Embedded Systems Security for Windows treats sign-in attempts as abnormal activity.
Exclusions	Not applied.	You can specify users and IP addresses which will not trigger the heuristic analyzer.
Task start schedule	First run is not scheduled.	You can configure settings to start the task on a schedule.

Managing Log Inspection rules via the Administration Plug-in

In this section, learn how to add and configure Log Inspection rules via the Administration Plug-in.

Configuring predefined task rules

Perform the following actions to configure the predefined rules for the Log Inspection task:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure application settings.
3. Perform one of the following actions in the details pane of the selected administration group:
   - To configure application settings for a group of protected devices, select the **Policies** tab and open the **Properties: <Policy name>** window.
   - To configure the settings of a task or application for an individual protected device, select the **Devices** tab and go to local task settings or application settings.
4. In the **System inspection** section, click the **Log Inspection** button in the **Settings** subsection.
   The **Log Inspection** window opens.
5. Select the **Predefined rules** tab.
6. Select or clear the **Apply predefined rules for log inspection** check box.

   For the task to run, at least one Log Inspection rule must be selected.

7. Select the rules you want to apply from the list of predefined rules:
   - There are patterns of a possible brute-force attack in the system.
   - There are patterns of a possible Windows Event log abuse.
   - Atypical actions detected on behalf of a new service installed.
   - Atypical logon that uses explicit credentials detected.
   - There are patterns of a possible Kerberos forged PAC (MS14-068) attack in the system.
   - Atypical actions detected directed at a privileged built-in group Administrators.
   - There is an atypical activity detected during a network logon session.
8. To configure the selected rules, click the **Advanced settings** button.
   The **Log Inspection** window opens.
9. In the **Brute-force attack detection** section, set the number of attempts and time frame used as triggers by the heuristic analyzer.
10. In the **Network logon detection** section, specify the start and end of the time interval. Kaspersky Embedded Systems Security for Windows considers logon attempts made during this interval to be as anomalous activity.
11. Select the **Exclusions** tab.

12. Perform the following actions to add trusted users:

    a. Click the **Browse** button.

    b. Select a user.

    c. Click the **OK** button.

    The selected user is added to the list of trusted users.

13. Perform the following actions to add trusted IP addresses:

    a. Enter the IP address.

    b. Click the **Add** button.

14. The entered IP address is added to the list of trusted IP addresses.

15. On the **Task management** tab, configure the task start schedule.

16. Click the **OK** button in the **Log Inspection** window.

The Log Inspection task configuration is saved.

Adding Log Inspection rules via the Administration Plug-in

Perform the following actions to add and configure a new custom Log Inspection rule:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.

2. Select the administration group for which you want to configure application settings.

3. Perform one of the following actions in the details pane of the selected administration group:

    - To configure application settings for a group of protected devices, select the **Policies** tab and open the **Properties: <Policy name>** window.

    - To configure the settings of a task or application for an individual protected device, select the **Devices** tab and go to local task settings or application settings.

4. In the **System inspection** section, click the **Log Inspection** button in the **Settings** subsection.

    The **Log Inspection** window opens.

5. On the **Custom rules** tab, select or clear the **Apply custom rules for log inspection** check box.

    You can control whether the preset rules are applied for Log Inspection. Select the check boxes corresponding to the rules you want to apply to Log Inspection.

6. To add a new custom rule, click the **Add** button.

    The **Custom log inspection rule** window opens.

7. In the **General** section specify the following information about the new rule:

- **Rule name**
- **Inform about new entries in the Windows Event Log with the specified identifiers**

8. In the **Triggering criteria** section, specify the event IDs that will trigger the rule:
   a. Enter an ID.
   b. Click the **Add** button.
      The entered event ID is added to the list. You can add an unlimited number of identifiers to each rule.
9. Click the **OK** button.
   The Log Inspection rule is added to the list of rules.

Managing Log Inspection rules via the Application Console

In this section, learn how to add and configure Log Inspection rules via the Application Console.

Configuring predefined task rules

Perform the following actions to configure the heuristic analyzer for the Log Inspection task:

1. In the Application Console tree, expand the **System Inspection** node.
2. Select the **Log Inspection** child node.
3. Click the **Log Inspection** link in the results pane of the **Properties** node.
   The **Task settings** window appears.
4. Select the **Predefined rules** tab.
5. Select or clear the **Apply predefined rules for log inspection** check box.

   For the task to run, at least one Log Inspection rule must be selected.

6. Select the rules you want to apply from the list of predefined rules:
   - There are patterns of a possible brute-force attack in the system.
   - There are patterns of a possible Windows Event log abuse.
   - Atypical actions detected on behalf of a new service installed.
   - Atypical logon that uses explicit credentials detected.
   - There are patterns of a possible Kerberos forged PAC (MS14-068) attack in the system.
   - Atypical actions detected directed at a privileged built-in group Administrators.

- There is an atypical activity detected during a network logon session.

7. To configure the selected rules, go to the **Extended** tab.
8. In the **Brute-force attack detection** section, set the number of attempts and time frame used as triggers by the heuristic analyzer.
9. In the **Network logon** section, specify the start and end of the time interval. Kaspersky Embedded Systems Security for Windows considers logon attempts made during this interval to be as anomalous activity.
10. Select the **Exclusions** tab.
11. Perform the following actions to add trusted users:
    a. Click the **Browse** button.
    b. Select a user.
    c. Click the **OK** button.
    The selected user is added to the list of trusted users.
12. Perform the following actions to add trusted IP addresses:
    a. Enter the IP address.
    b. Click the **Add** button.
    The entered IP address is added to the list of trusted IP addresses.
13. Select the **Schedule** and **Advanced** tabs to configure the task start schedule.
14. Click the **OK** button in the **Task settings** window.
    The Log Inspection task configuration is saved.

Adding Log Inspection rules via the Application Console

To add and configure a new custom Log Inspection rule:

1. In the Application Console tree, expand the **System Inspection** node.
2. Select the **Log Inspection** child node.
3. In the results pane of the **Log Inspection** node, click the **Log inspection rules** link.
4. The **Log inspection rules** window opens.
5. Clear or select the **Apply custom rules for log inspection. The rules configured are not applied until the checkbox is selected** check box. The checksum is displayed in the task log.

> You can control whether the predefined rules are applied to the Log Inspection task. Select the check boxes corresponding to the rules you want to apply to Log Inspection.

6. To create a new custom rule:

   a. Enter the name of the new rule.

   b. Click the **Add** button.
   The created rule is added to the general rule list.

7. To configure any rule:

   a. Select a rule from the list.
   In the right area of the window, the **Description** tab displays general information about the rule.

   > The description for the new rule is blank.

   b. Select the **Rule settings** tab.

8. In the **General** section specify the following information about the new rule:

   - **Rule name**
   - **Log name**
   - **Inform about new entries in the Windows Event Log with the specified identifiers**

9. In the **Event identifiers** section specify the event IDs that will trigger the rule:

   a. Enter an event ID.

   b. Click the **Add** button.
   The entered event ID is added to the list. You can add an unlimited number of identifiers to each rule.

10. Click the **Save** button.
    The configured log inspection rules will be applied.

Managing Log Inspection rules via the Web Plug-in

To add and configure Log Inspection rules via the Web Plug-in:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.
2. Click the policy name you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.
4. Select the **System Inspection** section.
5. Click the **Settings** button in the **Log Inspection** subsection.
6. Configure the settings described in the table below.

Log Inspection task settings

Setting	Description
Apply custom rules for log inspection	You can enable, disable, add, or modify the custom rules. The setting is available on the table is with the list of custom rules.
Apply predefined rules for log inspection	You can enable or disable the heuristic analyzer, which detects abnormal activity on the protected device. The setting is available on the table is with the list of custom rules.
Detect brute-force attack if an incorrect password is entered with a frequency defined	You can set the number of attempts and time frame used, which will be considered as triggers by the heuristic analyzer.
Detect network logon, if logged on within a period defined	You can indicate the start and end of the time interval during which Kaspersky Embedded Systems Security for Windows treats sign-in attempts as abnormal activity.
Users Exclusions	You can specify users which will not trigger the heuristic analyzer.
Excluded IP Addresses	You can specify IP addresses which will not trigger the heuristic analyzer.
Task management	You can configure settings to start the task on a schedule.

On-Demand Scan

This section provides information about On-Demand Scan tasks, and instructions on configuring On-Demand Scan task settings and security settings on the protected device.

About On-Demand Scan tasks

Kaspersky Embedded Systems Security for Windows scans the specified area for viruses and other computer security threats. Kaspersky Embedded Systems Security for Windows scans protected device files, RAM, and autorun objects.

Kaspersky Embedded Systems Security for Windows provides the following On-Demand Scan tasks:

- The Scan at Operating System Startup task is performed every time Kaspersky Embedded Systems Security for Windows starts. Application scans boot sectors and master boot records of hard drives, removable drives, system memory, and process memory. Every time Kaspersky Embedded Systems Security for Windows runs the task, it creates a copy of non-infected boot sectors. If it detects a threat in those sectors the next time the task starts, it replaces them with the backup copy.

  The Scan at Operating System startup task is created automatically after installation. By default, the Notify only mode is applied. In this case, after you deploy Kaspersky Embedded Systems Security for Windows on the devices, you can enable the Scan at Operating System Startup task if no issues with system services were discovered during scan. If the application detects critical system services as infected or probably infected objects, the Notify only mode gives you time to figure out the reason and solve the issue. If the application applies the Perform recommended action mode, which calls the Disinfect. Remove, if disinfection fails action, disinfection or removal of the system files may result in critical issues with the operating system startup.

  > The Scan at Operating System Startup task might not be performed if a protected device wakes up after either sleep or hibernate mode. The task is performed only at protected device restart or start up after complete shut down.

- By default, the Critical Areas Scan task is performed weekly on a schedule. Kaspersky Embedded Systems Security for Windows scans objects in critical areas of the operating system: autorun objects, boot sectors and master boot records of hard drives and removable drives, system memory and process memory. The application scans files in system folders, for example, %windir%\system32. Kaspersky Embedded Systems Security for Windows applies security settings that correspond to the Recommended level. You can modify the settings of the Critical Areas Scan task.

- The Quarantine Scan task is executed by default according to a schedule after every database update. The Quarantine Scan task scope cannot be modified.

- The Application Integrity Control task is performed daily. It provides the option of checking Kaspersky Embedded Systems Security for Windows modules for damage or modification. The application installation folder is checked. The task execution statistics indicate the number of modules checked and the number of modules found to be corrupted. The values of the task settings are defined by default and cannot be edited. The task start schedule settings can be edited.

Additionally, you can create custom On-Demand Scan tasks, for example, a task for scanning shared folders on the protected device.

Kaspersky Embedded Systems Security for Windows may run several On-Demand Scan tasks at the same time.

About the task scan scope and security settings

In the Application Console, the scan scope of the selected On-Demand Scan task is displayed as a tree or in the list of the protected device file resources that Kaspersky Embedded Systems Security for Windows can control. By default, the network file resources of the protected device are displayed in a list-view mode.

In the Administration Plug-in only the list view is available.

To display network file resources in the tree-view mode in the Application Console,

open the drop down list in the **Scan scope settings** window upper left sector and select **Tree-view**.

The items or nodes are displayed in a list-view or in a tree-view mode of the protected device file resources as follows:

☑ The node is included in the scan scope.

☐ The node is excluded from the scan scope.

☑ At least one of the child nodes of this node is excluded from the scan scope, or the security settings of the child node(s) differ(s) from the setting of a parental node (for a tree-view mode only).

The ☑ icon is displayed if all child nodes are selected, but the parent node is not selected. In this case, changes in the composition of files and folders of the parent node are disregarded automatically when the scan scope for the selected child node is being created.

Using the Application Console, you can also add virtual drives to the scan scope. The names of the virtual nodes are displayed in blue font.

Security settings

In the selected On-Demand Scan task, the default security settings can be modified by configuring them as common settings for the entire protection or scan scope, or as different settings for different nodes or items in the device's file resource tree or list.

Security settings configured for the selected parent node are automatically applied to all child nodes. The security settings of the parent node are not applied to child nodes that are configured separately.

The settings for a selected scan scope or protection scope can be configured using one of the following methods:

- Select one of three predefined security levels (**Maximum performance**, **Recommended**, or **Maximum protection**).
- Manually change the security settings for the selected nodes or items in the tree or list of the protected device's file resources (the security level changes to **Custom**).

A set of node settings can be saved in a template in order to be applied later to other nodes.

Predefined scan scopes

The tree or list of protected device file resources for the selected On-Demand Scan task is displayed in the **Scan scope settings** window.

The file resource tree or list displays the nodes to which you have read-access based on the configured Microsoft Windows security settings.

Kaspersky Embedded Systems Security for Windows contains the following predefined scan scopes:

- **My Computer**. Kaspersky Embedded Systems Security for Windows scans the entire protected device.
- **Local hard drives**. Kaspersky Embedded Systems Security for Windows scans objects on a protected device hard drives. All hard drives, individual disks, folders or files can be included in or excluded from the scan scope.
- **Removable drives**. Kaspersky Embedded Systems Security for Windows scans files on external devices, such as CDs or removable drives. All removable drives, individual disks, folders or files can be included in or excluded from the scan scope.
- **Network**. Network folders or files can be added to the scan scope by specifying their path in UNC (Universal Naming Convention) format. The account used to start the task must have permissions to access the added network folders and files. By default, On-Demand Scan tasks run under the system account.

  Connected network drives will also not be displayed in the protected device's file resource tree. To include objects on network drives in the scan scope, specify the path to the folder that corresponds to the network drive in UNC format.

- **System memory**. Kaspersky Embedded Systems Security for Windows scans the executable files and modules of the processes running in the operating system when the scan is initiated.
- **Startup objects**. Kaspersky Embedded Systems Security for Windows scans objects referred to by registry keys and configuration files, for example WIN.INI or SYSTEM.INI, as well as the application's modules that are started automatically at protected device startup.
- **Shared folders**. You can include shared folders on the protected device in the scan scope.
- **Virtual drives**. Virtual folders, files, and drives connected to the protected device can be included in the scan scope, for example, common cluster drives.

  Virtual drives created using a SUBST command are not displayed in the protected device's file resource tree in the Application Console. In order to scan objects on a virtual drive, include the protected device folder associated with the virtual drive in the scan scope.

Standard scan scopes are displayed in the tree of network file resources by default. They can be added to the list of network file resources when it is created in the scan scope settings.

By default, On-Demand Scan tasks are run under the following scopes:

- Scan at Operating System Startup task:

- **Local hard drives**.
- **Removable drives**.
- **System memory**.

- Critical Areas Scan:
  - **Local hard drives** (excluding Windows folders)
  - **Removable drives**.
  - **System memory**.
  - **Startup objects**.
- Other tasks:
  - **Local hard drives** (excluding Windows folders)
  - **Removable drives**.
  - **System memory**.
  - **Startup objects**.
  - **Shared folders**.

Online storage file scanning

About cloud files

Kaspersky Embedded Systems Security for Windows can interact with Microsoft OneDrive cloud files. The application supports the new OneDrive Files On-Demand feature.

> Kaspersky Embedded Systems Security for Windows does not support other online storages.

OneDrive Files On-Demand helps you access all your OneDrive files without having to download all of them and use storage space on your device. You can download files to your hard drive when you need to.

When the OneDrive Files On-Demand feature is on, you see status icons next to each file in the **Status** column in File Explorer. Each file has one of the following statuses:

This status icon indicates that the file is *only available online*. Online-only files are not physically stored on your hard drive. You can't open online-only files when your device is not connected to the Internet.

This status icon indicates that a file is *locally available*. This happens when you open an online-only file and it downloads to your device. You can open a locally available file anytime, even without Internet access. To clear up space you can change the file back to online-only.

This status icon indicates that a file is *stored on your hard drive and is always available*.

Cloud file scanning

Kaspersky Embedded Systems Security for Windows can only scan cloud files that are stored locally on a protected device. Such OneDrive files have the and statuses. The files are skipped during scanning, since they are not physically located on the protected device.

> Kaspersky Embedded Systems Security for Windows does not automatically download files from the cloud during the scanning, even if they are included in the scan scope.

Cloud files are processed by several Kaspersky Embedded Systems Security for Windows tasks in various scenarios depending on the task type:

- Real-time cloud file scanning: you can add folders containing cloud files to the Real-Time File Protection task protection scope. A file is scanned when it is accessed by the user. If a file is accessed by the user, it is downloaded, becomes locally available, and its status changes to . This allows the file to be processed by the Real-Time File Protection task.
- On-demand cloud file scanning: you can add folders containing cloud files to the On-Demand Scan task's scan scope. The task scans files with the and statuses. If any files are found in the scope, they will be skipped during scanning and an informational event will be recorded in the task log, indicating that the scanned file is only a placeholder for a cloud file and does not exist on a local drive.
- Generating and using applications launch control rules: you can create allowing and denying rules for and files using the Rule Generator for Applications Launch Control task. The Applications Launch Control task applies the Default Deny principle and created rules to process and block cloud files.

  > The Applications Launch Control task blocks the start of all cloud files, irrespective of their status. The files are not included in the rule generation scope by the application, as they are not physically stored on your hard drive. Since allowing rules cannot be created for such files, they are subject to the Default Deny principle.

When a threat is detected in a OneDrive cloud file, the application applies the action specified in the settings of the task performing the scanning. Thus, the file may be removed, disinfected, moved to quarantine, or backed up.

> Changes to local files are synchronized with the copies stored on OneDrive in accordance with the principles outlined in the relevant Microsoft OneDrive documentation.

About predefined security levels

> The **Use iChecker technology**, **Use iSwift technology**, **Use heuristic analyzer**, and **Check Microsoft signature in files** security settings are not included in the settings for the preset security levels. If the **Use iChecker technology**, **Use iSwift technology**, **Use heuristic analyzer**, and **Check Microsoft signature in files** settings change, the preset security level you have selected will not change.

You can apply one of the following three predefined security levels to a node selected in the device's file resource tree: **Maximum performance**, **Recommended**, and **Maximum protection**. Each of these levels contains its own predefined security settings (see the table below).

Maximum performance

The **Maximum performance** security level is recommended if your network has additional protected device security measures, for example, firewalls and existing security policies, beyond using Kaspersky Embedded Systems Security for Windows on protected devices.

Recommended

The **Recommended** security level ensures the best combination of protection and performance impact on devices. Kaspersky experts recommend this level as adequate to protect devices on most corporate networks. The **Recommended** security level is set by default.

Maximum protection

The **Maximum protection** security level is recommended if your organization's network has elevated device security requirements.

Predefined security levels and corresponding security setting values

Options	Security level		
	Maximum performance	Recommended	Maximum protection
Scan objects	By format	All objects	All objects
Scan only new and modified files	Enabled	Disabled	Disabled
Action to perform on infected and other objects	Disinfect. Remove, if disinfection fails	Perform action recommended by Kaspersky experts	Disinfect. Remove, if disinfection fails
System-critical objects are files required for the operation of the operating system and Kaspersky Embedded Systems Security for Windows. These files can not be deleted. Processes associated with such objects cannot be terminated.			
Action to perform on probably infected objects	Quarantine.	Perform action recommended by Kaspersky experts	Quarantine.
Exclude files	No	No	No
Do not detect	No	No	No
Stop scanning if it takes longer than (sec.)	60 sec.	No	No
Do not scan compound objects larger than (MB)	8 MB	No	No
Scan alternate NTFS streams	Yes	Yes	Yes
Scan disk boot sectors	Yes	Yes	Yes

and MBR			
Scan of compound objects	• SFX archives* • Packed objects* • Embedded OLE objects* * New and modified objects only	• Archives* • SFX archives* • Packed objects* • Embedded OLE objects* * All objects	• Archives* • SFX archives* • Email databases* • Plain mail* • Packed objects* • Embedded OLE objects* * All objects

Removable Drives Scan

You can configure scanning of removable drives connected to the protected device via a USB port.

Kaspersky Embedded Systems Security for Windows scans a removable drive using the On-Demand Scan task. The application automatically creates a new On-Demand Scan task when the removable drive is connected and deletes the task after the scanning is completed. The created task is performed with the predefined security level defined for removable drive scanning. You cannot configure the settings of the temporary On-Demand Scan task.

If you installed Kaspersky Embedded Systems Security for Windows without anti-virus databases, the removable drives scan will be unavailable.

Kaspersky Embedded Systems Security for Windows scans connected removable drives when they are registered as USB external devices in the operating system. The application does not scan a removable drive if the connection is blocked by the Device Control task. The application does not scan MTP-connected mobile devices.

Kaspersky Embedded Systems Security for Windows allows access to removable drives during scanning.

Scan results for each removable drive are available in the task log for the On-Demand Scan task created when the removable drive is connected.

You can change the settings of the Removable Drives Scan component (see the table below).

Removable Drives Scan settings

Setting	Default value	Description
Scan removable drives on connection via USB	Cleared	You can turn on or turn off scanning of removable drive upon connection to the protected device via USB.
Scan removable drives if its stored	8192 MB	You can reduce the component's scope by setting the maximum volume of data on the scanned drive.

data volume does not exceed (MB)		Kaspersky Embedded Systems Security for Windows does not scan a removable drive if the volume of stored data exceeds the specified value.
Scan with security level	Maximum protection	You can configure created On-Demand Scan tasks by selecting one of three security levels: • **Maximum protection** • **Recommended** • **Maximum performance** The algorithm used when infected, probably infected, and other objects are detected, as well as the other scan settings for each security level, correspond to the predefined security levels in the On-Demand Scan tasks.

About the Baseline File Integrity Monitor task

During the Baseline File Integrity Monitor task, Kaspersky Embedded Systems Security for Windows does not check locked files, folders, file shortcuts and cloud files.

The Baseline File Integrity Monitor task monitors the integrity of files in the monitoring scope by comparing the files' hash (MD5 hash or SHA256 hash) to a baseline.

On the first Baseline File Integrity Monitor task run, Kaspersky Embedded Systems Security for Windows creates a baseline by calculating and storing hash for files in the task's monitoring scope. If a Baseline File Integrity Monitor task monitoring scope was changed, Kaspersky Embedded Systems Security for Windows updates the baseline on the next Baseline File Integrity Monitor task run by calculating and storing hash for files in the task's monitoring scope. If a Baseline File Integrity Monitor task was deleted, Kaspersky Embedded Systems Security for Windows deletes the baseline for this Baseline File Integrity Monitor task.

You can delete a baseline without deleting the Baseline File Integrity Monitor task by using the command line.

The Baseline File Integrity Monitor task tracks the following changes of files in the monitoring scope:

- the monitoring scope contains file which is not present in the baseline
- the monitoring scope does not contain a file present in the baseline
- the hash of a file in the monitoring scope differs from the hash of this file in a baseline

The Baseline File Integrity Monitor task does not track changes to file's attributes and alternative streams.

If a file or a folder is inaccessible, Kaspersky Embedded Systems Security for Windows will not add this file or folder to the baseline during the baseline creation and will create an event about a failure to calculate file's checksum during the run of the Baseline File Integrity Monitor task.

A file or a folder may be inaccessible for the following reasons:

- the specified path does not exist
- a type of files specified by mask is not present under the specified path
- the specified file is locked
- the specified file is empty

Enabling start of On-Demand Scan task from context menu

You can enable the start of On-Demand Scan task for one or several files from a context menu in Microsoft Windows Explorer.

To enable the start of On-Demand Scan task from a context menu:

1. Create the following REG files:

```
Windows Registry Editor Version 5.0.0

[HKEY_CLASSES_ROOT\Directory\shell\kess\command]

@="C:\\Temp\\scan.cmd \"%1\""

[HKEY_CLASSES_ROOT\*\shell\kess\command]

@="C:\\Temp\\scan.cmd \"%1\""

[HKEY_CLASSES_ROOT\Directory\shell\kess]

@="Scan with Kaspersky Embedded Systems Security for Windows\"

"Icon"="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems Security\\kavtrayr.dll\",0"

[HKEY_CLASSES_ROOT\Directory\shell\kess\DefaultIcon]

@="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems Security\\kavtrayr.dll\",0"

[HKEY_CLASSES_ROOT\*\shell\kess]

@="Scan with Kaspersky Embedded Systems Security for Windows\"

"Icon"="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems Security\\kavtrayr.dll\",0"

[HKEY_CLASSES_ROOT\*\shell\kess\DefaultIcon]
@="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems Security\\kavtrayr.dll\",0"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers]

"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems Security\\kavshell.exe"="~ RUNASADMIN"
```

> You need to specify the actual location of the Kaspersky Embedded Systems Security for Windows installation folder.

2. Create the `scan.cmd` file with the following content:

```
@echo off
set LOGNAME=%RANDOM%
```

```
"C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security\kavshell.exe"
scan "%~1" /W:c:\temp\%LOGNAME%.txt

echo Scanning is in progress...
type c:\temp\%LOGNAME%.txt
del c:\temp\%LOGNAME%.txt

timeout /t -1
```

The `scan.cmd` file must contain the following information:

- The location of `kavshell.exe` file.
- The location of temporary file containing the scan results.
- Parameters for the `KAVSHELL SCAN` command.
- The timeout value for closing the console window when the task is finished.

3. Copy the `scan.cmd` file to the folder specified in the `[HKEY_CLASSES_ROOT\Directory\shell\kess\command]` REG file.

   The `C:\Temp` folder is used in example.

You don't need to restart the operating system.

Default On-Demand Scan tasks settings

By default On-Demand Scan tasks have the settings described in the table below. You can configure local system and custom On-Demand Scan tasks.

Default On-Demand Scan tasks settings

Setting	Default value	Description
Scan scope	Applied in local system and custom tasks: • **Scan at Operating System Startup**: the entire protected device, excluding shared folders and autorun objects. • **Critical Areas Scan**: the entire protected device,	You can change the scan scope. The scan scope cannot be configured for the **Quarantine Scan** and **Application Integrity Control** local system tasks. The **Scan at Operating System Startup** task is created automatically after installation. By default, the **Notify only** mode is applied. In this case, after you deploy Kaspersky Embedded Systems Security for Windows on the devices, you can enable the **Scan at Operating System Startup** task if no issues with system services were discovered during scan. If the application detects critical system services as infected or probably infected objects, the **Notify only** mode gives you time to figure out the reason and solve the issue. If the application applies the **Perform recommended action** mode, which calls the **Disinfect. Remove, if disinfection fails** . Disinfection or removal of the system files may result in critical issues with operating system startup.

	excluding shared folders and certain operating system files. • **On-Demand Scan** (custom tasks): the entire protected device.	
Security settings	Common settings for the entire scan scope correspond to the **Recommended** security level.	For nodes selected in the protected device's file resource list or tree, you can: • Select a different predefined security level • Manually change security settings You can save a group of security settings for a selected node as a template to use later for a different node.
Use heuristic analyzer	It is used with the **Medium** analysis level for Critical Areas Scan, Scan at Operating System Startup, and custom tasks. It is used with the **Deep** analysis level for the Quarantine Scan task.	Heuristic Analyzer can be enabled or disabled and the analysis level can be configured. The Quarantine Scan task analysis level cannot be configured. Heuristic Analyzer is not used in the Application Integrity Control and Baseline File Integrity Monitor tasks.
Apply Trusted Zone	Applied (Not applied for Quarantine Scan task)	General list of exclusions that can be used in selected tasks.
Use KSN for scanning	Applied.	You can improve your device's protection using the Kaspersky Security Network cloud service infrastructure.
Settings to start a task with specific permissions	The task is started under a system account.	You can edit settings to start tasks with specific account permissions for all system and custom On-Demand Scan tasks, except Quarantine Scan and Application Integrity Control tasks.
Perform	Not applied	You can configure the priority level of On-Demand Scan tasks.

task in background mode (low priority)		
Task start schedule	Applied in local system tasks: • Scan at Operating System Startup - **At application launch** • Critical Areas Scan - **Weekly** • Quarantine Scan - **After application database update** • Application Integrity Control - **Daily** Not used in newly created custom tasks.	You can configure the settings for scheduled task startup.
Registering scan execution and updating the device protection status	The device protection status is updated weekly after the Critical Areas Scan is performed.	You can configure settings for registering the execution of the Critical Areas Scan in the following ways: • Edit the settings of the Critical Areas Scan task start schedule. • Edit the scan scope of the Critical Areas Scan task. • Create custom On-Demand Scan tasks.

Managing On-Demand Scan tasks via the Administration Plug-in

In this section, learn how to navigate the Administration Plug-In interface and configure task settings for one or all protected devices on the network.

Navigation

Learn how to navigate to the required task settings via the chosen interface.

Opening the On-Demand Scan task wizard

To start creating a new custom On-Demand Scan task:

1. To create a local task:

   a. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console.

   b. Select the administration group that the protected device belongs to.

   c. In the results pane, on the **Devices** tab open the context menu for the protected device.

   d. Select the **Properties** menu option.

   e. In the window that opens, click the **Add** button in the **Tasks** section.

   The **New Task Wizard** window opens.

2. To create a group task:

   a. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.

   b. Select the administration group for which you want to create a task.

   c. Open the **Tasks** tab.

   d. Click the **New task** button.

   The **New Task Wizard** window opens.

3. To create a task for a custom group of protected device:

   a. In the **Device selections** node in the Kaspersky Security Center Administration Console tree, click the **Run selection** button to perform a device selection.

   b. Open the **Selection results "selection name"** tab.

   c. In the **Perform selection** drop-down list, select the **Create a task for a selection result** option.

   The **New Task Wizard** window opens.

4. Select the **On-Demand Scan** task in the list of available tasks for Kaspersky Embedded Systems Security for Windows.

5. Click the **Next** button.

   The **Settings** window opens.

Configure the task settings as required.

To configure an existing On-Demand Scan task,

double-click the task name in the list of Kaspersky Security Center tasks.

The **Properties: On-Demand Scan** window opens.

Opening the On-Demand Scan task properties

To open the application properties for the On-Demand Scan task for a single protected device:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group that the protected device belongs to.
3. Select the **Devices** tab.
4. Double-click the name of the protected device for which you want to configure the scan scope.
   The **Properties: <Protected device name>** window opens.
5. Select the **Tasks** section.
6. In the list of tasks created for the device, select the On-Demand Scan task that you created.
7. Click the **Properties** button.
   The **Properties: On-Demand Scan** window opens.

Configure the task settings as required.

Creating an On-Demand Scan task

To start creating a new custom On-Demand Scan task:

1. Open the **Settings** window in the New Task Wizard.
2. Select the required **Task creation method**.
3. Click the **Next** button.
4. Create a scan scope in the **Scan scope** window:

   By default, the scan scope includes critical areas of the protected device. Scan scopes are marked in the table with the icon ☑. Excluded scan scopes are marked with the ☐ icon in the table.

   You can change the scan scope: add specific preset scan scopes, disks, folders, network objects and files and assign specific security settings for each scope added.

   - To exclude all critical areas from the scan, open the context menu on each of the lines and select the **Remove scope** option.
   - To include a predefined scan scope, disk, folder, network object, or file in the scan scope:

     a. Right-click the **Scan scope** table and select **Add scope** or click the **Add** button.

b. In the **Add objects to the scan scope** window, select a predefined scope in the **Predefined scope** list, specify the protected device drive, folder, network object, or file on the protected device or on another protected device in the network, and click the **OK** button.

- To exclude subfolders or files from the scan, select the added folder (disk) in the **Scan scope** window of the wizard:

  a. Open the context menu and select the **Configure** option.

  b. Click the **Settings** button in the **Security level** window.

  c. On the **General** tab in the **On-demand scan settings** window clear the **Subfolders** and **Subfiles** check boxes.

- To change scan scope security settings:

  a. Open the context menu on the scope whose settings you wish to configure, and select **Configure**.

  b. In the **On-demand scan settings** window, select one of the predefined security levels, or click the **Settings** button to configure security settings manually.

  Security settings are configured the same way as for the Real-Time File Protection task.

- To skip embedded objects in the added scan scope:

  a. Open the context menu on the **Scan scope** table, select **Add exclusion**.

  b. Specify the objects to exclude: select a predefined scope in the **Predefined scope** list, and specify the protected device disk, folder, network object, or file on the protected device or on another protected device in the network.

  c. Click the **OK** button.

5. In the **Options** window, configure the heuristic analyzer and integration with other components:

   - Configure use of the heuristic analyzer.
   - Select the **Apply Trusted Zone** check box, if you want to exclude objects added to the Trusted Zone list from the scan scope of the task.
   - Select the **Use KSN for scanning** check box, if you want to use Kaspersky Security Network cloud services for the task.
   - To assign *Low* priority to the working process in which the task will be executed, select the **Perform task in background mode** check box in the **Options** window.

     By default, the working processes in which Kaspersky Embedded Systems Security for Windows tasks are run have *Medium* (Normal) priority.

   - To use the created task as a Critical Areas Scan task, select the **Consider task as critical areas scan** check box in the **Options** window.

6. Click the **Next** button.

7. In the **Schedule** window, specify the task start schedule settings.
8. Click the **Next** button.
9. In the **Selecting an account to run the task** window, specify the account you want to use.
10. Click the **Next** button.
11. Enter the task name.
12. Click the **Next** button.

    The task name should be no longer than 100 characters and cannot contain the following symbols: " * < > & \ : |

    The **Finish creating the task** window opens.
13. Click the **Finish** button to finish creating the task.

The new On-Demand Scan task will be created for the selected protected device or a group of protected devices.

Assigning the Critical Areas Scan status to an On-Demand Scan task

By default, Kaspersky Security Center assigns the *Warning* status to the protected device if the Critical Areas Scan task is performed less often than specified by the *Critical areas scan has not been performed for a long time* event-generation threshold in Kaspersky Embedded Systems Security for Windows.

To configure scanning of all protected devices in a single administration group:

1. Create a group On-Demand Scan task.
2. In the **Options** window of the task wizard, select the **Consider task as critical areas scan** check box. The specified task settings (the scan scope and security settings) will be applied to all protected devices in the group. Configure the task schedule.

   You can select the **Consider task as critical areas scan** check box when creating the On-Demand Scan task for a group of protected devices or later in the **Properties: <Task name>** window.
3. Using a new or existing policy, disable the scheduled start of On-Demand Scan local system tasks on the group protected devices.

Kaspersky Security Center Administration Server will then evaluate the security status of the protected device and will notify you about it based on the results of the last run of a task with the Critical Areas Scan status, rather than based on the results of the Critical Areas Scan local system task.

You can assign the *Critical Areas Scan* status both to On-Demand Scan group tasks and to tasks for groups of protected devices.

The Application Console can be used to view whether an On-Demand Scan task is a Critical Areas Scan task.

In the Application Console, the **Consider task as critical areas scan** check box is displayed in the task properties but cannot be edited.

Running an On-Demand Scan task in the background

By default the processes in which Kaspersky Embedded Systems Security for Windows tasks are executed are assigned the *Medium (Normal)* priority.

A process that will run an On-Demand Scan task can be assigned *Low* priority. Demoting the process priority increases the time required to execute the task, but may have a beneficial effect on the performance of the processes of other running programs.

Multiple background tasks can be running in a single worker process with low priority. You can specify the maximum number of processes for On-Demand Scan background tasks.

To change the priority of an existing On-Demand Scan task:

1. Open the **Properties: On-Demand Scan** window.
2. Select or clear the **Perform task in background mode** check box.
3. Click the **OK** button.

Configured task settings are saved and applied immediately to a running task. If the task is not running, the modified settings are applied at next start.

Registering execution of a Critical Areas Scan

By default, the device protection status is displayed in the results pane of the **Kaspersky Embedded Systems Security for Windows** node and is updated weekly after the Critical Areas Scan task is performed.

The time when the device protection status is updated is linked to the schedule of the On-Demand Scan task for which the **Consider task as critical areas scan** check box is selected. By default, the check box is selected only for the Critical Areas Scan task and cannot be modified for this task.

You can select the On-Demand Scan task linked to the device's protection status only from Kaspersky Security Center.

Configuring the task scan scope

If you modify the scan scope in the Scan at Operating System Startup and Critical Areas Scan tasks, you can restore the default scan scope in these tasks by repairing Kaspersky Embedded Systems Security for Windows itself (**Start** > **Programs** > **Kaspersky Embedded Systems Security for Windows** > **Modify or Remove Kaspersky Embedded Systems Security for Windows**). In the setup wizard, select **Repair installed components** and click **Next**. Then select the **Restore recommended application settings** check box.

To configure a scan scope for an existing On-Demand Scan task:

1. Open the **Properties: On-Demand Scan** window.
2. Select the **Scan scope** tab.
3. To include items in the scan scope:
   a. Open the context menu in an empty part of the scan scope list.
   b. Select the **Add scope** option in the context menu.
   c. In the opened **Add objects to the scan scope** window select an object type that you want to add:
      - **Predefined scope** – to add one of the predefined scopes on a protected device. Then in the drop-down list, select the desired scan scope.
      - **Disk, folder or network location** – to include an individual drive, folder or network object in the scan scope. Then select the desired scope by clicking the **Browse** button.
      - **File** – to include an individual file in the scan scope. Then select the desired scope by clicking the **Browse** button.

   You cannot add an object to a scan scope if it has already been added as an exclusion from scan scope.
4. To exclude individual nodes from the scan scope, clear the check boxes next to the names of these nodes or take the following steps:
   a. Open the context menu on the scan scope by right-clicking it.
   b. In the context menu, select the **Add exclusion** option.
   c. In the **Add exclusion** window, select an object type that you want to add as an exclusion from the scan scope following the procedure used when adding an object to the scan scope.
5. To modify the scan scope or an added exclusion, select the **Edit scope** option in the context menu for the corresponding scan scope.
6. To hide a previously added scan scope or exclusion in the list of network file resources, select the **Remove scope** option in the context menu for the necessary scan scope.

   The scan scope is excluded from the On-Demand Scan task scope when it is removed from the network file resource list.
7. Click the **OK** button.

The scan scope settings window closes. The newly configured settings are saved.

Selecting predefined security levels for On-Demand Scan tasks

You can apply one of the following three predefined security levels to a node selected in the protected device's file resource list: **Maximum performance**, **Recommended**, and **Maximum protection**.

To select one of the predefined security levels:

1. Open the **Properties: On-Demand Scan** window.
2. Select the **Scan scope** tab.
3. In the list of the protected device's list, select an item included in the scan scope in order to set a predefined security level.
4. Click the **Configure** button.

   The **On-demand scan settings** window opens.
5. On the **Security level** tab select the security level to be applied.

   The window displays the list of security settings corresponding to the security level selected.
6. Click the **OK** button.
7. Click the **OK** button in the **Properties: On-Demand Scan** window.

   Configured task settings are saved and applied immediately to a running task. If the task is not running, the modified settings are applied at next start.

Configuring security settings manually

By default, On-Demand Scan tasks use common security settings for the entire scan scope.

These settings correspond to the **Recommended** predefined security level.

The default values of security settings can be modified by configuring them as common settings for the entire scan scope or as different settings for different items in the protected device's file resource list or nodes in the tree.

To configure security settings manually:

1. Open the **Properties: On-Demand Scan** window.
2. Select the **Scan scope** tab.
3. Select the items in the scan scope list whose security settings you want to configure.

   A predefined security settings template can be applied for a selected node or item in the scan scope.
4. Click the **Configure** button.

   The **On-demand scan settings** window opens.
5. On the following tabs configure the security settings of the selected node or item in accordance with your requirements:

   - **General**
   - **Actions**
   - **Performance**

- **Hierarchical storage**

6. Click the **OK** button in the **On-demand scan settings** window.
7. Click the **OK** button in the **Scan scope** window.

The new scan scope settings are saved.

Configuring general task settings

To configure general On-Demand Scan task settings:

1. Open the **Properties: On-Demand Scan** window.
2. Select the **Scan scope** tab.
3. Click the **Configure** button.

   The **On-demand scan settings** window opens.
4. Click the **Settings** button.
5. On the **General** tab, in the **Scan objects** group box, specify the object types that you want to include in the scan scope:
   - **Objects to scan**:
     - **All objects**
     - **Objects scanned by format**
     - **Objects scanned according to list of extensions specified in anti-virus database**
     - **Objects scanned by specified list of extensions**
   - **Subfolders**
   - **Subfiles**
   - **Scan disk boot sectors and MBR**
   - **Scan alternate NTFS streams**
6. In the **Performance** group box, select or clear the **Scan only new and modified files** check box.

   To switch between available options when the check box is cleared, click on the **All** / **Only new** link for each of the compound object types.
7. In the **Scan of compound objects** group box, specify the compound objects that you want to include in the scan scope:
   - **All** / **Only new archives**

- All / Only new SFX archives
- All / Only new email databases
- All / Only new packed objects
- All / Only new plain email
- All / Only new embedded OLE objects

8. Click the **OK** button.

The new task configuration will be saved.

Configuring actions

To configure actions on infected and other detected objects during the On-Demand Scan task:

1. Open the Properties: On-Demand Scan window.
2. Select the **Scan scope** tab.
3. Click the **Configure** button.
   The **On-demand scan settings** window opens.
4. Click the **Settings** button.
5. Select the **Actions** tab.
6. Select the action to be performed on infected and other detected objects:
   - Notify only.
   - **Disinfect**.
   - **Disinfect. Remove if disinfection fails**.
   - Remove.
   - **Perform recommended action**.
7. Select the action to be performed on probably infected objects:
   - Notify only.
   - **Quarantine**.
   - Remove.
   - Perform recommended action.
8. Configure actions to be performed on objects depending on the type of object detected:
   a. Clear or select the Perform actions depending on the type of object detected check box.

b. Click the **Settings** button.

c. In the window that opens, select a primary action and a secondary action (to be performed if the primary action fails) for each type of detected object.

d. Click the **OK** button.

9. Select the action to perform on incurable compound objects: select or clear the **Entirely remove compound file that cannot be modified by the application in case of embedded object detection** check box.

10. Click the **OK** button.

The new task configuration will be saved.

Configuring performance

To configure performance settings for the On-Demand Scan task:

1. Open the **Properties: On-Demand Scan** window.
2. Select the **Scan scope** tab.
3. Click the **Configure** button.
   The **On-demand scan settings** window opens.
4. Click the **Settings** button.
5. Select the **Performance** tab.
6. In the **Exclusions** block:
   - Clear or select the **Exclude files** check box.
   - Clear or select the **Do not detect** check box.
   - Click the **Edit** button for each setting to add exclusions.
7. In the **Advanced settings** block:
   - **Stop scanning if it takes longer than (sec.)**
   - **Do not scan compound objects larger than (MB)**
   - **Use iSwift technology**
   - **Use iChecker technology**
8. Click the **OK** button.

The new task configuration will be saved.

Configuring Removable Drives Scan

To configure scanning of removable drives upon connection to the protected device:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure the task.
3. Select the **Policies** tab.
4. Double-click the policy name you want to configure.

   In the **Properties: <Policy name>** window that opens, select the **Supplementary** section.
5. Click the **Settings** button in the **Removable Drives Scan** subsection.

   The **Removable Drives Scan** window opens.
6. In the **Scan on connection** block, do the following:

   - Select the **Scan removable drives on connection via USB** check box, if you want Kaspersky Embedded Systems Security for Windows to automatically scan removable drives when they are connected.
   - If required, select the **Scan removable drives if its stored data volume does not exceed (MB)** and specify the maximum value in the field on the right.
   - In the **Scan with security level** drop-down list, specify the security level with the settings that you want for Removable Drive Scan tasks.
7. Click the **OK** button.

The specified settings are saved and applied.

Configuring a Baseline File Integrity Monitor task

To configure the Baseline File Integrity Monitor group task:

1. In the Kaspersky Security Center Administration Console tree, expand the **Managed devices** node and select the administration group for which you want to configure the application tasks.
2. In the details pane of a selected administration group, open the **Tasks** tab.
3. In the list of previously created group tasks, select a task you want to configure.
4. Open the **Properties: <Task name>** window in one of the following ways:

   - Double-click the name of the task in the list of created tasks.
   - Select the name of the task in the list of created tasks and click the **Configure task** link.
   - Open the context menu of the task name in the list of created tasks and select the **Properties** item.

   In the **Notification** section, configure the task event notification settings. For detailed information on configuring settings in this section, see *Kaspersky Security Center Help*.
5. In the **Scan scope** section do the following:

   a. To include folder in the Baseline File Integrity Monitor task scope:

1. Click the **Add** button.

   The **Scan area properties** window opens.

2. Select or clear the **Scan this area** check box.

3. Click the **Browse** button to specify the folder that you want to include in the Baseline File Integrity Monitor task scope.

4. Select the **Also scan subfolders** check box, if you want to include all subfolders in the Baseline File Integrity Monitor task scope.

b. To include or exclude the folder previously added to the Baseline File Integrity Monitor task scope select or clear the check box to the left of the folder's path in the **Scan scope** table.

c. To delete the folder previously added to the Baseline File Integrity Monitor task scope select this folder in the **Scan scope** table and click the **Delete** button.

6. Configure the task schedule in the **Schedule** section (you can configure a schedule for all task types except Rollback of Database Update).

7. In the **Account** section, specify the account whose rights will be used to run the task.

8. If required, specify the objects to exclude from the task scope in the **Exclusions from task scope** section.

   For detailed information on configuring settings in these sections, see *Kaspersky Security Center Help*.

9. Click the **OK** button in the **Properties: <Task name>** window.

   The newly configured group task settings are saved.

Managing On-Demand Scan tasks via the Application Console

In this section, learn how to navigate the Application Console interface and configure task settings on a protected device.

Navigation

Learn how to navigate to the required task settings via the chosen interface.

Opening the On-Demand Scan task settings

To open the general settings of the On-Demand Scan task via the Application Console:

1. Expand the **On-Demand Scan** node in the Application Console tree.

2. Select the child node that corresponds to the task that you want to configure.

3. In the child node results pane click the **Properties** link.

   The **Task settings** window appears.

Opening the On-Demand Scan task scope settings

To open the scan scope settings window via the Application Console:

1. Expand the **On-Demand Scan** node in the Application Console tree.
2. Select the child node corresponding to an On-Demand Scan task that you want to configure.
3. In the results pane of the selected node click the **Configure scan scope** link.

   The **Scan scope settings** window opens.

Creating and configuring an On-Demand Scan task

Custom tasks for a single protected device can be created in the **On-Demand Scan** node. Custom tasks cannot be created in the other functional components of Kaspersky Embedded Systems Security for Windows.

To create and configure a new On-Demand Scan task:

1. In the Application Console tree, open the context menu of the **On-Demand Scan** node.
2. Select **Add task**.

   The **Add task** window opens.
3. Configure the following task settings:

   - **Name** – A task name consisting of no more than 100 characters. It may contain any symbols except **" * < > & \ : |**.

     > You cannot save a task or configure a new task on the **Schedule**, **Advanced** and **Run as** tabs if the task name is not specified.

   - **Description** – additional information about the task, no more than 2000 characters. This information will be displayed in the task properties window.
   - **Use heuristic analyzer**.
   - **Perform task in background mode**.
   - **Apply Trusted Zone**.
   - **Consider task as critical areas scan**.
   - **Use KSN for scanning**.
4. Configure the task start schedule settings on the **Schedule** and **Advanced** tabs.

5. On the **Run as** tab, configure the settings to start the task using specific account permissions.
6. Click the **OK** button in the **Add task** window.

   A new custom On-Demand Scan task is created. A node with the name of the new task is displayed in the Application Console tree. The operation is recorded in the system audit log.
7. If required, in the results pane of the selected node, select **Configure scan scope**.

   The **Scan scope settings** window opens.
8. In the protected device's file resource tree or list, select the nodes or items that you want to include in the scan scope.
9. Select one of the predefined security levels or configure the scan settings manually.
10. Click the **Save** button in the **Scan scope settings** window.

The configured settings are applied at the next task start.

Scan scope in On-Demand Scan tasks

This section contains information on creating and using a scan scope in On-Demand Scan tasks.

Configuring the view for network file resources

To select the view for network file resources during configuration of scan scope settings:

1. Open the **Scan scope settings** window.
2. Open the drop-down list in the upper left section of the window and select one of the following options:
   - Select the **Tree-view** option to display the network file resources as a tree.
   - Select the **List-view** option to display the network file resources as a list.

   By default, the network file resources of the protected device are displayed in a list-view mode.
3. Click the **Save** button.

Creating a scan scope

If you are remotely managing Kaspersky Embedded Systems Security for Windows on the protected device using the Application Console installed on an administrator's workstation, you must be a member of administrators group on the protected device to be able to view folders on it.

The names of settings may vary depending on the installed Windows operating system.

If you modify the scan scope in the Scan at Operating System Startup and Critical Areas Scan tasks, you can restore the default scan scope in these tasks by repairing Kaspersky Embedded Systems Security for Windows itself (**Start** > **Programs** > **Kaspersky Embedded Systems Security for Windows** > **Modify or Remove Kaspersky Embedded Systems Security for Windows**). In the setup wizard, select **Repair installed components** and click **Next**. Then select the **Restore recommended application settings** check box.

The procedure of creating an On-Demand Scan task scope depends on the selected view of network file resources. You can configure the view of network file resources as a tree or as a list (default view).

To create a scan scope using the network file resource tree:

1. Open the **Scan scope settings** window.
2. In the left section of the window, open the network file resource tree to display all the nodes and child nodes.
3. Do the following:
   - To exclude individual nodes from the scan scope, clear the check boxes next to the names of these nodes.
   - To include individual nodes in the scan scope, clear the **My Computer** check box and do the following:
     - If all drives of a particular type are to be included in the scan scope, select the check box next to the name of the required drive type (for example, to add all removable drives on the protected device, select the **Removable drives** check box).
     - If an individual drive of a particular type is to be included in the scan scope, expand the node that contains drives of that type and select the check box next to the name of the required drive. For example, to select the removable drive **F:**, expand the **Removable drives** node and select the check box for the **F:** drive.
     - If you would like to include only a single folder or file on the drive, select the check box next to the name of that folder or file.
4. Click the **Save** button.

The **Scan scope settings** window will be closed. The newly configured settings are saved.

To create a scan scope using the network file resource list:

1. Open the **Scan scope settings** window.
2. To include individual nodes in the scan scope, clear the **My Computer** check box and do the following:
   a. Open the context menu on the scan scope by right-clicking it.
   b. In the context menu of the button, select **Add scan scope**.
   c. In the opened **Add scan scope** window, select the type of object that you want to add:
      - **Predefined scope**, if you want the scan scope to include one of the predefined scopes on the protected device. Then in the drop-down list, select the desired scan scope.
      - **Disk, folder or network location** – to include an individual drive, folder or network object in the scan scope. Then select the desired scope by clicking the **Browse** button.

- **File** – to include an individual file in the scan scope. Then select the desired scope by clicking the **Browse** button.

> You cannot add an object to a scan scope if it has already been added as an exclusion from scan scope.

3. To exclude individual nodes from the scan scope, clear the check boxes next to the names of these nodes or take the following steps:

   a. Open the context menu on the scan scope by right-clicking it.

   b. In the context menu, select the **Add exclusion** option.

   c. In the **Add exclusion** window, select an object type that you want to add as an exclusion from the scan scope following the procedure used when adding an object to the scan scope.

4. To modify the scan scope or an exclusion added, select the **Edit scope** option in the context menu for the necessary scan scope.

5. To hide a previously added scan scope or exclusion in the list of network file resources, select the **Remove from the list** option in the context menu for the necessary scan scope.

> The scan scope is excluded from the On-Demand Scan task scope when it is removed from the network file resource list.

6. Click the **Save** button.

The **Scan scope settings** window will be closed. The newly configured settings are saved.

Including network objects in the scan scope

Network drives, folders or files can be added to the scan scope by specifying their path in UNC (Universal Naming Convention) format.

> You can scan network folders under the system account.

To add a network location to the scan scope:

1. Open the **Scan scope settings** window.

2. Open the drop-down list in the upper left part of the window and select **Tree-view**.

3. In the context menu of the **Network** node:

   - Select **Add network folder**, if you want to add a network folder to the scan scope.

   - Select **Add network file**, if you want to add a network file to the scan scope.

4. Enter the path to the network folder or file in UNC format and press the **ENTER** key.

5. Select the check box next to the newly added network object to include it in the scan scope.

6. If necessary, change the security settings for the added network object.
7. Click the **Save** button.

The specified task settings are saved.

Creating a virtual scan scope

Virtual drives, folders, and files can be included in the scan scope in order to create a virtual scan scope.

> You can expand the scan scope by adding individual virtual drives, folders, or files only if the scan scope is viewed as a file resources tree.

To add a virtual drive to the scan scope:

1. Open the **Scan scope settings** window.
2. Open the drop-down list in the upper left part of the window and select **Tree-view**.
3. In the protected device's file resource tree, open the context menu of the **Virtual drives** node, click **Add virtual drive** and select the name of the virtual drive from the list of available names.
4. Select the check box next to the added drive in order to include the drive in the scan scope.
5. Click the **Save** button.

The specified task settings are saved.

To add a virtual folder or virtual file to the scan scope:

1. Open the **Scan scope settings** window.
2. Open the drop-down list in the upper left part of the window and select **Tree-view**.
3. In the protected device's file resource tree, open the context menu of the node to add a folder or file, and select one of the following options:
   - **Add virtual folder**, if you want to add a virtual folder to the scan scope.
   - **Add virtual file**, if you want to add a virtual file to the scan scope.
4. In the entry field specify the name of the folder or file.
5. In the line with the name of the folder or file, select the check box to include this folder or file in the scan scope.
6. Click the **Save** button.

The specified task settings are saved.

Configuring security settings

By default, On-Demand Scan tasks use common security settings for the entire scan scope.

These settings correspond to the **Recommended** predefined security level.

The default values of security settings can be modified by configuring them as common settings for the entire scan scope or as different settings for different items in the protected device's file resource list or nodes in the tree.

When working with the network file resource tree, security settings that are configured for the selected parent node are automatically applied to all child nodes. The security settings of the parent node are not applied to child nodes that are configured separately.

To manually configure security settings:

1. Open the **Scan scope settings** window.
2. In the left part of the window, select the node or item whose security settings you want to configure.

   A predefined security settings template can be applied for a selected node or item in the scan scope.

   In the left part of the window, you can select the view for network file resources, create a scan scope, or create a virtual scan scope.
3. In the right part of the window, do one of the following:
   - On the **Security level** tab select the security level to be applied.
   - On the following tabs configure the security settings of the selected node or item in accordance with your requirements:
     - **General**
     - **Actions**
     - **Performance**
     - **Hierarchical storage**
4. Click the **Save** button in the **Scan scope settings** window.

The new scan scope settings are saved.

Selecting predefined security levels for On-Demand Scan tasks

You can apply one of the following three predefined security levels to a node selected in the protected device's file resource tree or list: **Maximum performance**, **Recommended**, and **Maximum protection**.

To select one of the predefined security levels:

1. Open the **Scan scope settings** window.
2. In the protected device's network file resource tree or list, select a node or item to set the predefined security level.
3. Make sure that the selected node or item is included in the scan scope.

4. In the right part of the window, on the **Security level** tab select the security level to be applied.

   The window displays the list of security settings corresponding to the selected security level.

5. Click the **Save** button.

   The task settings are saved and applied immediately to the running task. If the task is not running, the modified settings are applied at the next start.

Configuring general task settings

To configure the general security settings of the On-Demand Scan task:

1. Open the **Scan scope settings** window.
2. Open the **General** tab.
3. In the **Scan objects** group box, specify the object types that you want to include in the scan scope:
   - **Objects to scan**:
     - **All objects**
     - **Objects scanned by format**
     - **Objects scanned according to list of extensions specified in anti-virus database**
     - **Objects scanned by specified list of extensions**
   - **Scan disk boot sectors and MBR**
   - **Scan alternate NTFS streams**
4. In the **Performance** group box, select or clear the **Scan only new and modified files** check box.

   To switch between available options when the check box is cleared, click on the **All** / **Only new** link for each of the compound object types.

5. In the **Scan of compound objects** group box, specify the compound objects that you want to include in the scan scope:
   - **All** / **Only new archives**
   - **All** / **Only new SFX archives**
   - **All** / **Only new email databases**
   - **All** / **Only new packed objects**
   - **All** / **Only new plain email**
   - **All** / **Only new embedded OLE objects**

6. Click the **Save** button.

The new task configuration will be saved.

Configuring actions

To configure the actions on infected and other detected objects for the On-Demand Scan task:

1. Open the **Scan scope settings** window.
2. Select the **Actions** tab.
3. Select the action to be performed on infected and other detected objects:
   - **Notify only**.
   - **Disinfect**.
   - **Disinfect. Remove if disinfection fails**.**Disinfect. Remove if disinfection fails**.
   - **Remove**.
   - **Perform recommended action**.
4. Select the action to be performed on probably infected objects:
   - **Notify only**.
   - **Quarantine**.
   - **Remove**.
   - **Perform recommended action**.
5. Configure actions to be performed on objects depending on the type of object detected:
   a. Clear or select the **Perform actions depending on the type of object detected** check box.
   b. Click the **Settings** button.
   c. In the window that opens, select a primary action and a secondary action (to be performed if the primary action fails) for each type of detected object.
   d. Click the **OK** button.
6. Select the action to perform on incurable compound objects: select or clear the **Entirely remove compound file that cannot be modified by the application in case of embedded object detection** check box.
7. Click the **Save** button.

The new task configuration will be saved.

Configuring performance

To configure performance settings for the On-Demand Scan task:

1. Open the **Scan scope settings** window.
2. Select the **Performance** tab.
3. In the **Exclusions** block:
   - Clear or select the **Exclude files** check box.
   - Clear or select the **Do not detect** check box.
   - Click the **Edit** button for each setting to add exclusions.
4. In the **Advanced settings** block:
   - **Stop scanning if it takes longer than (sec.)**
   - **Do not scan compound objects larger than (MB)**
   - **Use iSwift technology**
   - **Use iChecker technology**
5. Click the **Save** button.

The new task configuration will be saved.

Configuring hierarchical storage

To configure the actions on infected and other detected objects for the On-Demand Scan task:

1. Open the **Scan scope settings** window.
2. Select the **Hierarchical storage** tab.
3. Select the action to be performed on the files:
   - **Do not scan**
   - **Scan resident part of file only**
   - **Scan entire file**

     If this action is selected, you can specify the following options:
     - Select or clear the **Only if the file has been accessed within the specified period (days)** check box and specify the number of days.
     - Select or clear the **Do not copy file to a local hard drive, if possible** check box.
4. Click the **Save** button.

The new task configuration will be saved.

Removable Drives Scan

To configure scanning of the removable drives upon connection to the protected device in the Application Console:

1. In the Application Console tree, open the context menu of the **Kaspersky Embedded Systems Security for Windows** node and select the **Configure removable drives scan settings** option.

   The **Removable Drives Scan** window opens.

2. In the **Scan on connection** block, do the following:

   - Select the **Scan removable drives on connection via USB** check box, if you want Kaspersky Embedded Systems Security for Windows to automatically scan removable drives when they are connected.
   - If required, select the **Scan removable drives if its stored data volume does not exceed (MB)** and specify the maximum value in the field on the right.
   - In the **Scan with security level** drop-down list, specify the security level with the settings that you want for Removable Drive Scan tasks.

3. Click the **OK** button.

The specified settings are saved and applied.

On-Demand Scan task statistics

While the On-Demand Scan task is being executed, you can view information about the number of objects processed by Kaspersky Embedded Systems Security for Windows since it was started.

This information remains available even if the task is paused. You can view the task statistics in the task log.

To view the statistics of an On-Demand Scan task:

1. Expand the **On-Demand Scan** node in the Application Console tree.
2. Select the On-Demand Scan task whose statistics you want to view.

Task statistics are displayed in the **Statistics** section of the results pane of the selected node.

Information about objects processed by Kaspersky Embedded Systems Security for Windows since it was started is presented in the table below.

On-Demand Scan task statistics

Field	Description
Detected	Number of objects detected by Kaspersky Embedded Systems Security for Windows. For example, if Kaspersky Embedded Systems Security for Windows detects one malicious object in five files, the value in this field increases by one.
Infected and other	Number of objects that Kaspersky Embedded Systems Security for Windows found and classified as infected or number of found legitimate software files that were not excluded

objects detected	from the scan scope and were classified as legitimate software that can be used by intruders to damage your device or personal data.
Probably infected objects detected	Number of objects found by Kaspersky Embedded Systems Security for Windows to be probably infected.
Objects not disinfected	Number of objects that Kaspersky Embedded Systems Security for Windows did not disinfect for the following reasons: • The detected object is of a type that cannot be disinfected. • An error occurred during disinfection.
Objects not moved to Quarantine	Number of objects that Kaspersky Embedded Systems Security for Windows attempted to quarantine unsuccessfully, for example, due to insufficient disk space.
Objects not removed	Number of objects that Kaspersky Embedded Systems Security for Windows attempted to delete unsuccessfully, because, for example, access to the object was blocked by another application.
Objects not scanned	Number of objects in the protection scope that Kaspersky Embedded Systems Security for Windows failed to scan, because, for example, access to the object was blocked by another application.
Objects not backed up	Number of objects whose copies Kaspersky Embedded Systems Security for Windows attempted to save in Backup unsuccessfully, for example, due to insufficient disk space.
Processing errors	Number of objects whose processing resulted in an error.
Objects disinfected	Number of objects disinfected by Kaspersky Embedded Systems Security for Windows.
Moved to Quarantine	Number of objects quarantined by Kaspersky Embedded Systems Security for Windows.
Moved to Backup	Number of objects whose copies Kaspersky Embedded Systems Security for Windows saved to Backup.
Objects removed	Number of objects removed by Kaspersky Embedded Systems Security for Windows.
Password-protected objects	Number of objects (archives, for example) that Kaspersky Embedded Systems Security for Windows skipped because they were password protected.
Corrupted objects	Number of objects skipped by Kaspersky Embedded Systems Security for Windows because their format was corrupted.
Objects processed	Total number of objects processed by Kaspersky Embedded Systems Security for Windows.

You can also view the On-Demand Scan task statistics in the selected task log by clicking the **Open task log** link in the **Management** section of the results pane.

We recommend that you manually process the events recorded on the **Events** tab in the task log upon task completion.

Creating and configuring a Baseline File Integrity Monitor task

To create or configure a new Baseline File Integrity Monitor task:

1. In the Application Console tree, open the context menu of the **System Inspection** node.
2. Select **Create Baseline File Integrity Monitor task**.

   The **Add task** window opens.
3. In the **Hash calculation algorithm** drop-down list, select one of the options:
   - **MD5**
   - **SHA256**
4. In the **Scan areas** table do the following:
   a. To add a file or folder in the Baseline File Integrity Monitor task scope:
      1. Click the **Add** button.

         The **Scan area properties** window opens.
      2. Select or clear the **Scan this area** check box.
      3. Click the **Browse** button to specify the file or folder that you want to include in the Baseline File Integrity Monitor task scope.
      4. Select the **Also scan subfolders** check box, if you want to include all subfolders in the Baseline File Integrity Monitor task scope.
      5. Click the **OK** button.

   b. To change a file or folder previously added to the Baseline File Integrity Monitor task scope:
      1. Click the **Change** button.

         The **Scan area properties** window opens.
      2. Select or clear the **Scan this area** check box.
      3. Click the **Browse** button to specify the file or folder that you want to include in the Baseline File Integrity Monitor task scope.
      4. Select or clear the **Also scan subfolders** check box, if you want to include or exclude all subfolders from the Baseline File Integrity Monitor task scope.
      5. Click the **OK** button.

   c. To delete the file or folder previously added to the Baseline File Integrity Monitor task scope select this file or folder in the **Scan areas** table and click the **Remove** button.
5. Configure the task start schedule settings on the **Schedule** and **Advanced** tabs.
6. On the **Run as** tab, configure the settings to start the task using specific account permissions.

7. Click the **OK** button in the **Add task** window.

   A new custom Baseline File Integrity Monitor task is created. A node with the name of the new task is displayed in the Application Console tree. The operation is recorded in the system audit log.

To open the settings of the Baseline File Integrity Monitor task:

1. In the Application Console tree, expand the **System Inspection** node.
2. Select the child node that corresponds to the task that you want to configure.
3. In the child node results pane click the **Properties** link.

   The **Task settings** window appears.

Managing On-Demand Scan tasks via the Web Plug-in

In this section, learn how to navigate the Web Plug-In interface for protected devices on the network.

Opening the On-Demand Scan task wizard

To start creating a new local On-Demand Scan task:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the **Groups** tab to select the administration group that the protected device belongs to.
3. Click the protected device name.
4. In the **<Device name>** window that opens select the **Tasks** tab.
5. Click the **Add** button.

   The **New Task Wizard** window opens.
6. In the **Application** drop-down list, select **Kaspersky Embedded Systems Security for Windows**.
7. In the **Task type** drop-down list select **On-Demand Scan** task.
8. Click the **Next** button.

Configure the task settings as required.

To start creating a new group On-Demand Scan task:

1. In the main window of the Web Console, select **Devices** → **Tasks**.
2. Click the **Groups** tab to select the administration group for which you want to create a task.
3. Click the **Add** button.

   The **New Task Wizard** window opens.
4. In the **Application** drop-down list, select **Kaspersky Embedded Systems Security for Windows**.

5. In the **Task type** drop-down list select **On-Demand Scan** task.
6. Click the **Next** button.

Configure the task settings as required.

To start creating a new On-Demand Scan task for a custom group:

1. In the main window of the Web Console, select **Devices** → **Device selections**.
2. Select the selection for which you want to create a task.
3. Click the **Start** button.
4. In the **Selection results** window, select the devices for which you want to create a task.
5. Click the **New task** button.
6. In the **Application** drop-down list, select **Kaspersky Embedded Systems Security for Windows**.
7. In the **Task type** drop-down list select **On-Demand Scan** task.
8. Click the **Next** button.

Configure the task settings as required.

To configure an existing On-Demand Scan task:

1. In the main window of the Web Console, select **Devices** → **Tasks**.
2. Click the task name in the list of Kaspersky Security Center tasks.

The **<Task name>** window opens.

Opening the On-Demand Scan task properties

To open the application properties for the On-Demand Scan task for a single protected device:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the **Groups** tab to select the administration group that the protected device belongs to.
3. Click the protected device name.
4. In the **<Device name>** window that opens select the **Tasks** tab.
5. In the list of tasks created for the device, select the On-Demand Scan task that you created.
6. Open the **Application settings** tab.

Configuring the task scan scope

To configure a scan scope for an existing On-Demand Scan task:

1. Open the On-Demand Scan task properties.
2. Select the **Scan scope** section.
3. Do one of the following:
   - Click the **Add** button to add a new rule.
   - Select an existing rule and click **Edit** button.

   The **Edit scope** window opens.
4. Switch the toggle button to **Active** and select an object type.
5. In the **Objects protection** section, configure the following settings:
   - **Objects protection mode**:
     - **All objects**
     - **Objects scanned by format**
     - **Objects scanned according to list of extensions specified in anti-virus database**
     - **Objects scanned by specified list of extensions**
   - **Subfolders**
   - **Subfiles**
   - **Scan disk boot sectors and MBR**
   - **Scan alternate NTFS streams**
   - Protect only new and modified files
6. In the **Compound objects protection** section, specify the compound objects that you want to include in the scan scope:
   - **Archives**
   - **SFX archives**
   - **Packed objects**
   - **Email databases**
   - **Plain email**
   - **Embedded OLE objects**
7. In the **Action to perform on infected and other objects** section, select the action to be performed on infected and other detected objects:

- Notify only
- Disinfect
- Disinfect. Remove if disinfection fails
- Remove
- Recommended

8. In the **Action to perform on probably infected objects** section, select the action to be performed on probably infected objects:
   - Notify only
   - Quarantine
   - Remove
   - Recommended
9. In the **Action to perform on probably infected objects** section, select or clear the Entirely remove compound file that cannot be modified by the application in case of embedded object detection check box.
10. In the **Exclusions** section, configure the following settings:
    - Clear or select the Exclude files check box.
    - Clear or select the Do not detect check box.
11. In the **Advanced settings** section, configure the following settings:
    - Stop scanning if it takes longer than (sec)
    - Do not scan compound objects larger than (MB)
    - Use iSwift technology
    - Use iChecker technology
12. In the **Action on the offline files** section, select the action to be performed on the files:
    - **Do not scan**
    - **Scan resident part of file only**
    - **Scan entire file**

      If this action is selected, you can specify the following options:

      - Select or clear the **Only if the file has been accessed within the specified period (days)** check box and specify the number of days.
      - Select or clear the **Do not copy file to a local hard drive, if possible** check box.
13. Click the **OK** button.

Configuring the task settings

To configure settings of an existing On-Demand Scan task:

1. Open the On-Demand Scan task properties.
2. Select the **Options** section.
3. Clear or select the **Use Heuristic Analyzer** check box.
4. If necessary, select the level of analysis using the **Heuristic analysis level** drop-down list.
5. In the **Integration with other components** section, configure the following settings:
   - Select the **Apply Trusted Zone** check box, if you want to exclude objects added to the Trusted Zone list from the scan scope of the task.
   - Select the **Use KSN for scanning** check box, if you want to use Kaspersky Security Network cloud services for the task.
   - To assign *Low* priority to the working process in which the task will be executed, select the **Perform task in background mode** check box.

     By default, the working processes in which Kaspersky Embedded Systems Security for Windows tasks are run have *Medium* (Normal) priority.

   - To use the created task as a Critical Areas Scan task, select the **Consider task as critical areas scan** check box.

Trusted zone

This section provides information about the Trusted Zone in Kaspersky Embedded Systems Security for Windows, as well as instructions on how to add objects to the Trusted Zone when running tasks.

About the Trusted Zone

The Trusted Zone is a list of exclusions from the protection or scan scope that you can generate and apply to On-Demand Scan and Real-Time File Protection tasks, newly created custom On-Demand Scan tasks, and all system On-Demand Scan tasks, except for the Quarantine Scan task.

The Trusted Zone is applied in Real-Time File Protection and On-Demand Scan tasks by default.

The list of rules for generating the Trusted Zone can be exported to an XML configuration file in order to then import it into Kaspersky Embedded Systems Security for Windows running on another protected device.

Trusted processes

Applies to the Real-Time File Protection tasks.

Some applications on the protected device may be unstable if the files that they access are intercepted by Kaspersky Embedded Systems Security for Windows. Such applications include, for example, system domain controller applications.

To avoid disrupting the operation of such applications, you can disable protection of files accessed by the running processes of these applications (thereby creating a list of trusted processes within the Trusted Zone).

Microsoft Corporation recommends excluding some Microsoft Windows operating system files and Microsoft application files from Real-Time File Protection as programs that cannot be infected. The names of some of these are listed on the Microsoft website (article code: KB822158).

You can enable or disable the use of trusted processes in the Trusted Zone.

> If an executable file is modified, for example, through an update, Kaspersky Embedded Systems Security for Windows will exclude it from the list of trusted processes.

The application does not use the file's path on a protected device to trust the process. The path to the file on the protected device is used only to search for the file, calculate a checksum, and provide the user with the information about the source of the executable file.

Backup operations

Applies to Real-Time Computer Protection tasks.

When data stored on hard drives is backed up to external devices, you can disable protection of objects that are accessed during the backup operations. Kaspersky Embedded Systems Security for Windows will scan objects which the backup application opens for reading with the FILE_FLAG_BACKUP_SEMANTICS attribute.

Exclusions

- Applies to Real-Time File Protection tasks.
- All detectable objects in the specified areas of the protected device.
- Specified detectable objects by name or name mask within the entire protection or scan scope.

Configuring Trusted Zone settings via the Administration Plug-in

This section describes how to configure a trusted zone for protected devices using the Administration Plug-in.

Adding exclusions

To add an exclusion to the Trusted Zone in the Kaspersky Security Center policy:

1. In the Administration Plug-in, go to the Trusted Zone settings in the policy that you want to configure.

   a. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.

   b. Select the administration group for which you want to configure the task.

   c. Select the **Policies** tab.

   d. Double-click the policy name you want to configure.

   e. In the **Properties: <Policy name>** window that opens, select the **Supplementary** section.

   f. In the **Trusted Zone** section, click **Settings**.

   The **Trusted Zone** window opens.

2. On the **Exclusions** tab, specify the objects to be skipped by Kaspersky Embedded Systems Security for Windows during scanning and protection:

   - To create recommended exclusions, click **Add recommended exclusions**.
   - To import preconfigured exclusions, click the **Import** button and, in the window that opens, select the configuration file in XML format stored on your device.

     Exclusions from the XML file will be added to the exclusion list.
   - To manually specify the conditions under which an object will be considered trusted, click the **Add** button and proceed to the next steps.

     The **Exclusion rule parameters** window opens.

3. If you clicked the **Add** button, in the **Object will not be scanned if the following conditions are met** section, specify the objects that you want to exclude from the protection / scan scope and objects that you want to exclude among detectable objects:

- If you want to exclude an object from the protection or scan scope:

  a. Select the **Object excluded from scanning** check box.

  b. Click the **Edit** button.

  The **Object to exclude from scanning** window opens.

  c. Specify the object that you want to exclude from the scan scope.

  > When specifying the objects, you can use names masks (via ? and * characters) and all types of environment variables. The resolving of environment variables (replacing variables with their values) is performed by Kaspersky Embedded Systems Security for Windows when starting a task, or when applying new settings to a running task (not applicable to On-Demand Scan tasks). Kaspersky Embedded Systems Security for Windows resolves environment variables under the account used to start the task. For more information on environment variables, refer to the Microsoft Knowledge Base.

  d. Click the **OK** button.

  e. Select the **Apply to subfolders** check box, if you want to exclude all child files and folders of the specified object from the protection or scan scope.

- If you want to specify the name of a detectable object:

  a. Select the **Objects excluded from detection** check box.

  b. Click the **Edit** button.

  The **Objects to exclude from detection** window opens.

  c. Specify the name or name mask of the detectable object according to the Virus Encyclopedia classification.

  d. Click the **Add** button.

  e. Click the **OK** button.

4. In the **Exclusion usage scope** block, select the check boxes next to the names of the tasks to which the exclusion should be applied.

5. Click the **OK** button.

   The added exclusions will be displayed in the **Trusted Zone** window, in the list on the **Exclusions** tab.

6. In the **Trusted Zone** window, click the **OK** button.

Adding trusted processes

To add one or more processes to the list of trusted processes using the Administration Plug-in:

1. In the Administration Plug-in, go to the Trusted Zone settings in the policy that you want to configure.

a. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.

b. Select the administration group for which you want to configure the task.

c. Select the **Policies** tab.

d. Double-click the policy name you want to configure.

e. In the **Properties: <Policy name>** window that opens, select the **Supplementary** section.

f. In the **Trusted Zone** section, click **Settings**.

The **Trusted Zone** window opens.

2. Select the **Trusted processes** tab.

3. Select the **Do not check file backup operations** check box to skip scanning of file read operations.

4. Select the **Do not check file activity of the specified processes** check box to skip file operation scanning for trusted processes.

5. To add prcesses to the list of trusted processes, do one of the following:

- To import preconfigured trusted processes, click the **Import** button and, in the window that opens, select the configuration file in XML format stored on your device.

  Processes from the XML file will be added to the list of trusted processes.

- To manually specify the processes, click the **Add** button and proceed to the next steps.

6. If you clicked the **Add** button, in the button's context menu, select one of the options:

- **Multiple processes**.

  In the **Adding trusted processes** window that opens, configure the following:

  a. **Use full process path on disk to consider it trusted**.

  b. **Use process file hash to consider it trusted**.

  c. Click the **Browse** button to add data based on executable processes.

  d. Select an executable file in the window that opens.

  > You can only add one executable file at a time. Repeat steps c-d to add other executable files.

  e. Click the **Processes** button to add data based on running processes.

  f. Select processes in the window that opens. To select multiple processes, press and hold the **CTRL** button while selecting.

  g. In the **Exclusion usage scope** block, select the check boxes next to the names of the tasks to which you want to apply exclusions.

h. Click the **OK** button.

The account under which the Real-Time File Protection task is run must have administrator rights on the device with Kaspersky Embedded Systems Security for Windows installed in order to allow viewing of the list of active processes. You can sort processes in the list of active processes by file name, process identifier (PID), or path to the executable file of the process on the protected device. Note, that you can select running processes by clicking the **Processes** button only using the Application Console on a protected device or in the specified host settings via the Kaspersky Security Center.

- **One process based on file name and path**.

  In the **Adding a process** window that opens, do the following:

  a. Enter a path to an executable file (including the file name).

  When specifying the objects, you can use names masks (via ? and * characters) and all types of environment variables. The resolving of environment variables (replacing variables with their values) is performed by Kaspersky Embedded Systems Security for Windows when starting a task, or when applying new settings to a running task (not applicable to On-Demand Scan tasks). Kaspersky Embedded Systems Security for Windows resolves environment variables under the account used to start the task. For more information on environment variables, refer to the Microsoft Knowledge Base.

  b. In the **Exclusion usage scope** block, select the check boxes next to the names of the tasks to which you want to apply exclusions.

  c. Click the **OK** button.

- **One process based on object properties**.

  In the **Trusted process adding** window that opens, configure the following:

  a. Click the **Browse** button to select a process.

  b. **Use full process path on disk to consider it trusted**.

  c. **Use process file hash to consider it trusted**.

  d. In the **Exclusion usage scope** block, select the check boxes next to the names of the tasks to which you want to apply exclusions.

  e. Click the **OK** button.

  To add the selected process to the list of trusted processes, at least one trust criterion must be selected.

If you made a process trusted for the Applications Launch Control task and created trusted distribution package from the executable file of this process in the task settings, the Trusted Zone settings have a higher priority. Kaspersky Embedded Systems Security for Windows considers the process to be trusted, but blocks execution of the executable file of this process.

7. In the **Trusted Zone** window, click the **OK** button.

The selected file or process will be added to the list of trusted processes in the **Trusted Zone** window.

Configuring certificate monitoring

You can configure monitoring of certificates used for signing applications.

To configure certificate monitoring via the Administration Plug-in:

1. In the Administration Plug-in, go to the Trusted Zone settings in the policy that you want to configure.

   a. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.

   b. Select the administration group for which you want to configure the task.

   c. Select the **Policies** tab.

   d. Double-click the policy name you want to configure.

   e. In the **Properties: <Policy name>** window that opens, select the **Supplementary** section.

   f. In the **Trusted Zone** section, click **Settings**.
   The **Trusted Zone** window opens.

2. Select the **Certificate monitoring** tab.

3. Select the **Enable certificate monitoring** check box if you want the application to apply certificate monitoring rules.

4. Specify the value of the **Notify about the expiration of the certificate** setting if you want the application to publish an event about the approaching certificate expiration date in the system audit log a specified number of days before expiry. The default is 30 days.

   The application publishes an event about the approaching certificate expiration date once before restarting the application or the protected device. The application does not publish an event when the software signed with a certificate with an approaching expiration date is started again, if the application or the protected devices have not been restarted.

5. Add certificate monitoring rules.

6. In the **Trusted Zone** window, click the **OK** button.

Kaspersky Embedded Systems Security for Windows applies the new certificate monitoring settings immediately. Information about the date and time when the settings were modified, and the values of the certificate monitoring settings before and after modification are saved to the system audit log.

Adding certificate monitoring rules

To add certificate monitoring rules via the Administration Plug-in:

1. In the Administration Plug-in, go to the Trusted Zone settings in the policy that you want to configure.

   a. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.

   b. Select the administration group for which you want to configure the task.

   c. Select the **Policies** tab.

   d. Double-click the policy name you want to configure.

   e. In the **Properties: <Policy name>** window that opens, select the **Supplementary** section.

   f. In the **Trusted Zone** section, click **Settings**.

   The **Trusted Zone** window opens.

2. Select the **Certificate monitoring** tab.

3. Add a certificate monitoring rule in one of the following ways:

   - Manually

     a. Click the **Add** button.

     The **Certificate monitoring rule settings** window opens.

     b. Set a rule-triggering criterion:

     - **Certificate subject mask**. The application applies the rule to certificates whose title (the value in the Subject field) matches the mask entered in the **Certificate subject mask** field.

       You can use the ? and * wildcards for any number of masked characters. Value verification is case-insensitive.

     - **Certificate thumbprint**. The application applies the rule for the certificate whose thumbprint matches the one specified in the **Certificate thumbprint** field.

       Certificate thumbprint verification is case-insensitive.

     c. If necessary, disable **Allow programs to run with an untrusted certificate**.

     d. If necessary, disable the **Publish event about certificate expiration** option.

     e. Click the **OK** button.

   - By importing an XML file with pre-configured certificate monitoring rules

a. Click the **Import** button.

b. In the standard Windows system window that opens, specify the path to the XML file.

c. Click the **Open** button.

The new certificate monitoring rule is displayed in the list on the **Certificate monitoring** tab.

4. In the **Trusted Zone** window, click the **OK** button.

Exporting certificate monitoring rules

To export certificate monitoring rules via the Administration Plug-in:

1. In the Administration Plug-in, go to the Trusted Zone settings in the policy that you want to configure.

   a. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.

   b. Select the administration group for which you want to configure the task.

   c. Select the **Policies** tab.

   d. Double-click the policy name you want to configure.

   e. In the **Properties: <Policy name>** window that opens, select the **Supplementary** section.

   f. In the **Trusted Zone** section, click **Settings**.
   The **Trusted Zone** window opens.

2. Select the **Certificate monitoring** tab.

3. Click the **Export** button.
   The standard Microsoft Windows **Save as** window opens.

4. In the window that opens, specify the XML file you want to export the rules to. If no such file exists, it will be created. If a file with the specified name already exists, its contents will be overwritten.

5. Click the **Save** button.

Certificate monitoring rules will be exported to the specified XML file.

Applying the not-a-virus mask

The *not-a-virus* mask makes it possible to skip scanning of legitimate software files that may be considered harmful. The mask affects the following tasks:

- Real-Time File Protection.

- On-Demand Scan

If the mask is not added to the exclusions list, Kaspersky Embedded Systems Security for Windows will apply the actions specified in the task settings to software that falls under the *not-a-virus* category.

To enable the use of the not-a-virus mask:

1. In the Administration Plug-in, go to the Trusted Zone settings in the policy that you want to configure.

   a. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.

   b. Select the administration group for which you want to configure the task.

   c. Select the **Policies** tab.

   d. Double-click the policy name you want to configure.

   e. In the **Properties: <Policy name>** window that opens, select the **Supplementary** section.

   f. In the **Trusted Zone** section, click **Settings**.

   The **Trusted Zone** window opens.

2. On the **Exclusions** tab, in the **Objects to detect** column, select the check box next to the *not-a-virus:** exclusion added to the trusted zone by default unless already selected.

3. Click the **OK** button.

Configuring the Trusted Zone via the Application Console

This section describes how to configure a trusted zone for a protected device via the Application Console.

If the protected device is being managed by an active Kaspersky Security Center policy, and the policy blocks changes to the application settings, these settings cannot be edited via the Application Console.

Adding an exclusion to the Trusted Zone

To manually add an exclusion to the trusted zone via the Application Console:

1. In the Application Console tree, open the context menu of the **Kaspersky Embedded Systems Security for Windows** node.

2. Select the **Configure Trusted Zone settings** menu option.

   The **Trusted Zone** window opens.

3. Select the **Exclusions** tab.

4. Specify the objects to be skipped by Kaspersky Embedded Systems Security for Windows during scanning and protection:

   - To import preconfigured exclusions, click the **Import** button and, in the window that opens, select the configuration file in XML format stored on your device.

     Exclusions from the XML file will be added to the exclusion list.

   - To manually specify the conditions under which an object will be considered trusted, click the **Add** button and proceed to the next steps.

     The **Exclusion rule parameters** window opens.

5. If you clicked the **Add** button, in the **Object will not be scanned if the following conditions are met** section, specify the objects that you want to exclude from the protection / scan scope and objects that you want to exclude among detectable objects:

   - If you want to exclude an object from the protection or scan scope:

     a. Select the **Object excluded from scanning** check box.

     b. Click the **Edit** button.

        The **Object to exclude from scanning** window opens.

     c. Specify the object that you want to exclude from the scan scope.

        When specifying the objects, you can use names masks (via ? and * characters) and all types of environment variables. The resolving of environment variables (replacing variables with their values) is performed by Kaspersky Embedded Systems Security for Windows when starting a task, or when applying new settings to a running task (not applicable to On-Demand Scan tasks). Kaspersky Embedded Systems Security for Windows resolves environment variables under the account used to start the task. For more information on environment variables, refer to the Microsoft Knowledge Base.

     d. Click the **OK** button.

     e. Select the **Apply to subfolders** check box, if you want to exclude all child files and folders of the specified object from the protection or scan scope.

   - If you want to specify the name of a detectable object:

     a. Select the **Objects excluded from detection** check box.

     b. Click the **Edit** button.

        The **Objects to exclude from detection** window opens.

     c. Specify the name or name mask of the detectable object according to the Virus Encyclopedia classification.

     d. Click the **Add** button.

     e. Click the **OK** button.

6. In the **Exclusion usage scope** block, select the check boxes next to the names of the tasks to which the exclusion should be applied.

7. Click the **OK** button.

   The added exclusions will be displayed in the **Trusted Zone** window, in the list on the **Exclusions** tab.

8. In the **Trusted Zone** window, click the **OK** button.

Adding trusted processes

You can add a process to the list of trusted processes using one of the following methods:

- Select the process from the list of processes running on the protected device.
- Select the executable file of a process regardless of whether the process is currently running.

> If the executable file of a process has been modified, Kaspersky Embedded Systems Security for Windows excludes this process from the list of trusted processes.

To add one or more processes to the list of trusted processes using the Application Console:

1. In the Application Console tree, open the context menu of the **Kaspersky Embedded Systems Security for Windows** node.
2. Select the **Configure Trusted Zone settings** menu option.

   The **Trusted Zone** window opens.

3. Select the **Trusted processes** tab.
4. Select the **Do not check file backup operations** check box to skip scanning of file read operations.
5. Select the **Do not check file activity of the specified processes** check box to skip file operation scanning for trusted processes.
6. To add prcesses to the list of trusted processes, do one of the following:

   - To import preconfigured trusted processes, click the **Import** button and, in the window that opens, select the configuration file in XML format stored on your device.

     Processes from the XML file will be added to the list of trusted processes.

   - To manually specify the processes, click the **Add** button and proceed to the next steps.

7. If you clicked the **Add** button, in the button's context menu, select one of the options:

   - **Multiple processes**.

     In the **Adding trusted processes** window that opens, configure the following:

     a. **Use full process path on disk to consider it trusted**.

     b. **Use process file hash to consider it trusted**.

     c. Click the **Browse** button to add data based on executable processes.

     d. Select an executable file in the window that opens.

You can only add one executable file at a time. Repeat steps c-d to add other executable files.

e. Click the **Processes** button to add data based on running processes.

f. Select processes in the window that opens. To select multiple processes, press and hold the **CTRL** button while selecting.

g. In the **Exclusion usage scope** block, select the check boxes next to the names of the tasks to which you want to apply exclusions.

h. Click the **OK** button.

The account under which the Real-Time File Protection task is run must have administrator rights on the device with Kaspersky Embedded Systems Security for Windows installed in order to allow viewing of the list of active processes. You can sort processes in the list of active processes by file name, process identifier (PID), or path to the executable file of the process on the protected device. Note, that you can select running processes by clicking the **Processes** button only using the Application Console on a protected device or in the specified host settings via the Kaspersky Security Center.

- **One process based on file name and path**.

  In the **Adding a process** window that opens, do the following:

  a. Enter a path to an executable file (including the file name).

  When specifying the objects, you can use names masks (via `?` and `*` characters) and all types of environment variables. The resolving of environment variables (replacing variables with their values) is performed by Kaspersky Embedded Systems Security for Windows when starting a task, or when applying new settings to a running task (not applicable to On-Demand Scan tasks). Kaspersky Embedded Systems Security for Windows resolves environment variables under the account used to start the task. For more information on environment variables, refer to the Microsoft Knowledge Base.

  b. In the **Exclusion usage scope** block, select the check boxes next to the names of the tasks to which you want to apply exclusions.

  c. Click the **OK** button.

- **One process based on object properties**.

  In the **Trusted process adding** window that opens, configure the following:

  a. Click the **Browse** button to select a process.

  b. Use full process path on disk to consider it trusted.

  c. Use process file hash to consider it trusted.

  d. In the **Exclusion usage scope** block, select the check boxes next to the names of the tasks to which you want to apply exclusions.

  e. Click the **OK** button.

To add the selected process to the list of trusted processes, at least one trust criterion must be selected.

If you made a process trusted for the Applications Launch Control task and created trusted distribution package from the executable file of this process in the task settings, the Trusted Zone settings have a higher priority. Kaspersky Embedded Systems Security for Windows considers the process to be trusted, but blocks execution of the executable file of this process.

8. In the **Trusted Zone** window, click the **OK** button.

The selected file or process will be added to the list of trusted processes in the **Trusted Zone** window.

Configuring certificate monitoring

You can configure monitoring of certificates used for signing applications.

To configure certificate monitoring via the Application Console:

1. In the Application Console tree, open the context menu of the **Kaspersky Embedded Systems Security for Windows** node.
2. Select the **Configure Trusted Zone settings** menu option.

   The **Trusted Zone** window opens.
3. Select the **Certificate monitoring** tab.
4. Select the **Enable certificate monitoring** check box if you want the application to apply certificate monitoring rules.
5. Specify the value of the **Notify about the expiration of the certificate** setting if you want the application to publish an event about the approaching certificate expiration date in the system audit log a specified number of days before expiry. The default is 30 days.

   The application publishes an event about the approaching certificate expiration date once before restarting the application or the protected device. The application does not publish an event when the software signed with a certificate with an approaching expiration date is started again, if the application or the protected devices have not been restarted.
6. Add certificate monitoring rules.
7. In the **Trusted Zone** window, click **Apply**.

Kaspersky Embedded Systems Security for Windows applies the new certificate monitoring settings immediately. Information about the date and time when the settings were modified, and the values of the certificate monitoring settings before and after modification are saved to the system audit log.

Adding certificate monitoring rules

To add certificate monitoring rules via the Application Console:

1. In the Application Console tree, open the context menu of the **Kaspersky Embedded Systems Security for Windows** node.
2. Select the **Configure Trusted Zone settings** menu option.

   The **Trusted Zone** window opens.
3. Select the **Certificate monitoring** tab.
4. Add a certificate monitoring rule in one of the following ways:

   - Manually

     a. Click the **Add** button.

     The **Certificate monitoring rule settings** window opens.

     b. Set a rule-triggering criterion:

     - **Certificate subject mask**. The application applies the rule to certificates whose title (the value in the Subject field) matches the mask entered in the **Certificate subject mask** field.

       You can use the ? and * wildcards for any number of masked characters. Value verification is case-insensitive.

     - **Certificate thumbprint**. The application applies the rule for the certificate whose thumbprint matches the one specified in the **Certificate thumbprint** field.

       Certificate thumbprint verification is case-insensitive.

     c. If necessary, disable **Allow programs to run with an untrusted certificate**.

     d. If necessary, disable the **Publish event about certificate expiration** option.

     e. Click the **OK** button.

   - By importing an XML file with pre-configured certificate monitoring rules

     a. Click the **Import** button.

     b. In the standard Windows system window that opens, specify the path to the XML file.

     c. Click the **Open** button.

   The new certificate monitoring rule is displayed in the list on the **Certificate monitoring** tab.
5. In the **Trusted Zone** window, click **Apply**.

Exporting certificate monitoring rules

To export certificate monitoring rules via the Application Console:

1. In the Application Console tree, open the context menu of the **Kaspersky Embedded Systems Security for Windows** node.
2. Select the **Configure Trusted Zone settings** menu option.

   The **Trusted Zone** window opens.
3. Select the **Certificate monitoring** tab.
4. Click the **Export** button.

   The standard Microsoft Windows **Save as** window opens.
5. In the window that opens, specify the XML file you want to export the rules to. If no such file exists, it will be created. If a file with the specified name already exists, its contents will be overwritten.
6. Click the **Save** button.

Certificate monitoring rules will be exported to the specified XML file.

Applying the not-a-virus mask

The *not-a-virus* mask makes it possible to skip scanning of legitimate software files that may be considered harmful. The mask affects the following tasks:

- Real-Time File Protection.
- On-Demand Scan

If the mask is not added to the exclusions list, Kaspersky Embedded Systems Security for Windows will apply the actions specified in the task settings to software that falls under the *not-a-virus* category.

To enable the use of the not-a-virus mask:

1. In the Application Console tree, open the context menu of the **Kaspersky Embedded Systems Security for Windows** node.
2. In the **Kaspersky Embedded Systems Security for Windows** node context menu, select **Configure Trusted Zone settings**.

   The **Trusted Zone** window opens.
3. On the **Exclusions** tab, in the **Objects to detect** column, select the check box next to the *not-a-virus:** exclusion added to the trusted zone by default unless already selected.
4. Click the **OK** button.

Configuring the Trusted Zone via the Web Plug-in

This section describes how to configure a trusted zone for protected devices via the Web Plug-in.

Adding exclusions

To add an exclusion to the Trusted Zone in the Kaspersky Security Center policy:

1. In the Web Plug-in, go to the Trusted Zone settings in the policy that you want to configure.

   a. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.

   b. Click the policy name you want to configure.

   c. In the **<Policy name>** window that opens, select the **Application settings** tab.

   d. Select the **Supplementary** section.

   e. In the **Trusted Zone** section, click **Settings**.

   A **Trusted Zone** window opens on the **Exclusions** tab.

2. On the **Exclusions** tab, use one of the following methods to specify the objects for Kaspersky Embedded Systems Security for Windows to skip during scanning and protection:

   - Manually

a. Click the **Add** button.

b. Select the **Object excluded from scanning** check box to specify further objects to be excluded from the protection or scan scope.

c. In the drop-down list, select the object type that you want to exclude from the scan scope.

When specifying the objects, you can use names masks (via ? and * characters) and all types of environment variables. The resolving of environment variables (replacing variables with their values) is performed by Kaspersky Embedded Systems Security for Windows when starting a task, or when applying new settings to a running task (not applicable to On-Demand Scan tasks). Kaspersky Embedded Systems Security for Windows resolves environment variables under the account used to start the task. For more information on environment variables, refer to the Microsoft Knowledge Base.

d. Select the **Apply to subfolders** check box to exclude all child folders of the specified object from the protection or scan scope.

e. Select the **Objects excluded from detection** check box to further specify objects to exclude from detection.

f. Specify the name or name mask of the object to detect according to the Virus Encyclopedia classification.

g. Select the check boxes next to the names of the tasks to apply the exclusion to.

h. Click the **OK** button.

- By importing an XML file with pre-configured exclusions

a. Click the **Import** button.

b. In the standard Windows system window that opens, specify the path to the XML file.

c. Click the **Open** button.

The new exclusions appear on the **Exclusions** tab.

3. In the **Trusted Zone** window, click the **OK** button.

Adding trusted processes

To add one or more processes to the list of trusted processes using the Administration Plug-in:

1. In the Web Plug-in, go to the Trusted Zone settings in the policy that you want to configure.

a. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.

b. Click the policy name you want to configure.

c. In the **<Policy name>** window that opens, select the **Application settings** tab.

d. Select the **Supplementary** section.

e. In the **Trusted Zone** section, click **Settings**.

A **Trusted Zone** window opens on the **Exclusions** tab.

2. Select the **Trusted processes** tab.

3. Select the **Do not check file backup operations** check box to skip scanning of file read operations.

4. Select the **Do not check file activity of the specified processes** check box to skip file operation scanning for trusted processes.

5. Add processes to the trusted list in one of the following ways:

- Manually

a. Click the **Add** button.

b. Enter the name of the executable file of the process that you want to add to the trusted list.

c. Select a trust criterion:

- **Full path**. The application will consider a process trusted if you enter the full path to its executable.
- **Hash**. The application will consider a process trusted if you enter a hash for its executable.
- **Full path and hash**. The application will consider a process trusted if you enter the full path to its executable and its hash.

d. Depending on the option selected at the previous step, enter the full path, hash, or the full path and hash for the executable file of the process that you want to add to the trusted list.

e. In the **Exclusion usage scope** block, select the check boxes next to the names of the tasks that you want to trust this process.

To add the selected process to the list of trusted processes, at least one trust criterion must be selected.

If you made a process trusted for the Applications Launch Control task and created a trusted distribution package from the executable file of this process in the task settings, the Trusted Zone settings will have a higher priority. Kaspersky Embedded Systems Security for Windows considers the process to be trusted, but blocks execution of the executable file of this process.

a. Click the **OK** button.

- By importing an XML file with process data

a. Click the **Import** button.

b. In the standard Windows system window that opens, specify the path to the XML file.

c. Click the **Open** button.

The trusted processes that have been added are displayed on the **Trusted processes** tab.

6. In the **Trusted Zone** window, click the **OK** button.

Configuring certificate monitoring

You can configure monitoring of certificates used for signing applications.

To configure certificate monitoring settings via the Web Plug-in:

1. In the Web Plug-in, go to the Trusted Zone settings in the policy that you want to configure.

    a. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.

    b. Click the policy name you want to configure.

    c. In the **<Policy name>** window that opens, select the **Application settings** tab.

    d. Select the **Supplementary** section.

    e. In the **Trusted Zone** section, click **Settings**.

    A **Trusted Zone** window opens on the **Exclusions** tab.

2. Select the **Certificate monitoring** tab.

3. Select the **Enable certificate monitoring** check box if you want the application to apply certificate monitoring rules.

4. Specify the value of the **Notify about the expiration of the certificate (1 - 99 days) in advance** setting if you want the application to publish an event about the approaching certificate expiration date in the system audit log the specified number of days before expiry. The default is 30 days.

    The application publishes an event about the approaching certificate expiration date once before restarting the application or the protected device. The application does not publish an event when the software signed with a certificate with an approaching expiration date is started again, if the application or the protected devices have not been restarted.

5. Add certificate monitoring rules.

6. In the **Trusted Zone** window, click the **OK** button.

Kaspersky Embedded Systems Security for Windows applies the new certificate monitoring settings immediately. Information about the date and time when the settings were modified, and the values of the certificate monitoring settings before and after modification are saved to the system audit log.

Adding certificate monitoring rules

To add certificate monitoring rules via the Web Plug-in:

1. In the Web Plug-in, go to the Trusted Zone settings in the policy that you want to configure.

a. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.

b. Click the policy name you want to configure.

c. In the **<Policy name>** window that opens, select the **Application settings** tab.

d. Select the **Supplementary** section.

e. In the **Trusted Zone** section, click **Settings**.

A **Trusted Zone** window opens on the **Exclusions** tab.

2. Select the **Certificate monitoring** tab.

3. Add a certificate monitoring rule in one of the following ways:

- Manually

  a. Click the **Add** button.

  A window opens with the certificate monitoring rule settings.

  b. If necessary, disable the rule by clearing the **Enable certificate monitoring** check box.

  c. Set a rule-triggering criterion:

  - **by certificate subject mask**. The application applies the rule to certificates whose title (the value in the Subject field) matches the mask entered in the **Certificate subject mask** field.

    You can use the ? and * wildcards for any number of masked characters. Value verification is case-insensitive.

  - **by certificate thumbprint**. The application applies the rule for the certificate whose thumbprint matches the one specified in the **Certificate thumbprint** field.

    Certificate thumbprint verification is case-insensitive.

  d. If necessary, disable **Allow programs to run with an untrusted certificate**.

  e. If necessary, disable the **Publish event about certificate expiration** option.

  f. Click the **OK** button.

- By importing an XML file with pre-configured certificate monitoring rules

  a. Click the **Import** button.

  b. In the standard Windows system window that opens, specify the path to the XML file.

  c. Click the **Open** button.

The new certificate monitoring rule is displayed in the list on the **Certificate monitoring** tab.

4. In the **Trusted Zone** window, click the **OK** button.

Exporting certificate monitoring rules

To export certificate monitoring rules via the Web Plug-in:

1. In the Web Plug-in, go to the Trusted Zone settings in the policy that you want to configure.

   a. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.

   b. Click the policy name you want to configure.

   c. In the **<Policy name>** window that opens, select the **Application settings** tab.

   d. Select the **Supplementary** section.

   e. In the **Trusted Zone** section, click **Settings**.

   A **Trusted Zone** window opens on the **Exclusions** tab.

2. Select the **Certificate monitoring** tab.

3. Click the **Export** button.

   The standard Microsoft Windows **Save as** window opens.

4. In the window that opens, specify the path to save the XML file that you want to export the certificate monitoring rules to.

5. Click the **Save** button.

The certificate monitoring rules will be saved to the MonitoringCertificates.xml file at the specified path.

Applying the not-a-virus mask

The *not-a-virus* mask makes it possible to skip scanning of legitimate software files that may be considered harmful. The mask affects the following tasks:

- Real-Time File Protection.
- On-Demand Scan

If the mask is not added to the exclusions list, Kaspersky Embedded Systems Security for Windows will apply the actions specified in the task settings to software that falls under the *not-a-virus* category.

To enable the use of the not-a-virus mask:

1. In the Web Plug-in, go to the Trusted Zone settings in the policy that you want to configure.

a. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.

b. Click the policy name you want to configure.

c. In the **<Policy name>** window that opens, select the **Application settings** tab.

d. Select the **Supplementary** section.

e. In the **Trusted Zone** section, click **Settings**.

A **Trusted Zone** window opens on the **Exclusions** tab.

2. On the **Exclusions** tab, in the **Objects to detect** column, select the check box next to the *not-a-virus:** exclusion added to the trusted zone by default unless already selected.

3. Click the **OK** button.

Exploit Prevention

This section contains instructions on how to configure process memory protection settings.

About Exploit Prevention

Kaspersky Embedded Systems Security for Windows provides the ability to protect process memory from exploits. This feature is implemented in the Exploit Prevention component. You can change the component's activity status and configure process memory protection settings.

The component protects process memory from exploits by inserting an external Process Protection Agent ("Protection Agent") in the protected process.

A Process Protection Agent is a dynamically loaded Kaspersky Embedded Systems Security for Windows module that is inserted in protected processes to monitor their integrity and reduce the risk of being exploited.

The Agent's operation within the protected process requires starting and stopping the process: the initial loading of the Agent into a process added to the protected process list is only possible if the process is restarted. Additionally, after a process has been removed from the protected process list, the Agent can be unloaded only after the process has been restarted.

The Agent must be stopped to unload it from protected processes: if the Exploit Prevention component is uninstalled, the application freezes the environment and forces the Agent to be unloaded from protected processes. If during uninstallation of the component Agent is inserted in any of the protected processes, you must terminate the affected process. A protected device restart may be required (for example, if system process is being protected).

If evidence of an exploit attack in a protected process is detected, Kaspersky Embedded Systems Security for Windows performs one of the following actions:

- Terminates the process if an exploit attempt is made.
- Reports the fact that the process has been compromised.

You can stop process protection using one of the following methods:

- Uninstalling the component.
- Removing the process from the list of protected processes and restarting the process.

Kaspersky Security Exploit Prevention Service

The Kaspersky Security Exploit Prevention Service is required on the protected device in order for the Exploit Prevention component to be most effective. This service and the Exploit Prevention component are part of the recommended installation. During installation of the service on the protected device, the kavfswh process is created and started. This communicates information about protected processes from the component to the Protection Agent.

After the Kaspersky Security Exploit Prevention Service is stopped, Kaspersky Embedded Systems Security for Windows continues to protect processes added to the protected process list, is also loaded in newly-added processes, and applies all available exploit prevention techniques to protect process memory.

If your device is running the Windows 10 operating system or later, the application will not continue to protect processes and process memory after the Kaspersky Security Exploit Prevention Service is stopped.

If the Kaspersky Security Exploit Prevention Service is stopped, the application will not receive information about events occurring with protected processes (including information about exploit attacks and the termination of processes). Furthermore, the Agent will not be able to receive information about new protection settings and the addition of new processes to the protected process list.

Exploit Prevention mode

You can select one of the following modes to configure actions taken to reduce risks that vulnerabilities will be exploited in protected processes:

- **Terminate on exploit**: apply this mode to terminate a process when an exploit attempt is made.

  Upon detecting an attempt to exploit a vulnerability in a protected critical operating system process, Kaspersky Embedded Systems Security for Windows does not terminate the process, regardless of the mode indicated in the Exploit Prevention component settings.

- **Notify only**: apply this mode to receive information about instances of exploits in protected processes using events in the Security log.

  If this mode is selected, Kaspersky Embedded Systems Security for Windows creates events to log all attempts to exploit vulnerabilities. Selected by default.

Managing Exploit Prevention via the Administration Plug-in

In this section, learn how to navigate the Administration Plug-In interface and configure the component settings for one or all protected devices on the network.

Navigation

Learn how to navigate to the required task settings via the chosen interface.

Opening policy settings for Exploit Prevention

To open the Exploit Prevention settings via the Kaspersky Security Center policy:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure the task.
3. Select the **Policies** tab.
4. Double-click the policy name you want to configure.

5. In the **Properties: <Policy name>** window that opens, select the **Real-Time Computer Protection** section.
6. Click **Settings** in the **Exploit prevention** subsection.
   The **Exploit Prevention** window opens.

Configure Exploit Prevention as required.

Opening the Exploit Prevention properties window

To open the properties window for Exploit Prevention:

1. Expand the **Managed devices** node in the Kaspersky Security Center Administration Console tree.
2. Select the administration group for which you want to configure the task.
3. Select the **Devices** tab.
4. Open the **Properties: <Protected device name>** window in one of the following ways:
   - Double-click the name of the protected device.
   - Open the context menu of the protected device name and select the **Properties** item.

   The **Properties: <Protected device name>** window opens.
5. In the **Applications** section, select **Kaspersky Embedded Systems Security 3.4 for Windows**.
6. Click the **Properties** button.
   The **Kaspersky Embedded Systems Security 3.4 for Windows Application settings** window opens.
7. Select the **Real-Time Computer Protection** section.
8. Click **Settings** in the **Exploit Prevention** subsection.
   The **Exploit Prevention** window opens.

Configure Exploit Prevention as required.

Configuring process memory protection settings

To configure Exploit Prevention settings for processes added to the list of protected processes, perform the following actions:

1. Open the Exploit Prevention window.
2. In the **Exploit prevention mode** block, configure the following settings:
   - Prevent vulnerable processes exploit.
     - Terminate on exploit.

- Notify only.

3. In the **Preventing actions** block, configure the following settings:

   - Notify about abused processes via Terminal Service.
   - Prevent vulnerable processes exploit even if Kaspersky Security Service is disabled.

4. Click the **OK** button in the **Exploit Prevention** window.

Kaspersky Embedded Systems Security for Windows saves and applies the configured process memory protection settings.

Adding a process to the protection scope

The Exploit Prevention component protects several processes by default. You can exclude the processes from the protection scope by clearing the corresponding check boxes in the list.

To add a process to the list of protected processes:

1. Open the Exploit Prevention window.
2. On the **Protected processes** tab, click the **Browse** button.

   A Microsoft Windows Explorer window opens.
3. Select the process you want to add to the list.
4. Click the **Open** button.

   The process name is displayed in the line.
5. Click the **Add** button.

   The process will be added to the list of protected processes.
6. Select the added process.
7. Click the **Set exploit prevention techniques** button.

   The **Exploit prevention techniques** window opens.
8. Select one of the options for applying impact reduction techniques:

   - **Apply all available exploit prevention techniques**.

     If this option is selected, the list cannot be edited. By default, all available techniques are applied to a process.
   - **Apply selected exploit prevention techniques**

     If this option is selected, you can edit the list of impact reduction techniques applied:

     a. Select the check boxes next to the techniques that you want to apply to protect the selected process.

     b. Select or clear the **Apply Attack Surface Reduction technique** check box.
9. Configure settings for the Attack Surface Reduction technique:

- Enter the names of the modules whose launch will be blocked from the protected process in the **Deny modules** field.
- In the **Do not deny modules if launched in the Internet Zone** field, select the check boxes next to the options for which you want to allow modules to be launched:
  - **Internet**
  - **Local intranet**
  - **Trusted URL**
  - **Restricted URL**
  - **Computer**

  These settings only apply to Internet Explorer®.

10. Click the **OK** button.

The process is added to the task protection scope.

Managing Exploit Prevention via the Application Console

In this section, learn how to navigate the Application Console interface and configure the component settings on a protected device.

Navigation

Learn how to navigate to the required task settings via the chosen interface.

Opening the Exploit Prevention general settings

*To open the **Exploit Prevention settings** window:*

1. Expand the **Real-Time File Protection** node in the Application Console tree.
2. Select the **Exploit Prevention** node.
3. In the Processes protection settings section, click the **Properties** link.
   The **Exploit Prevention settings** window opens.

Configure general settings for Exploit Prevention as required.

Opening the Exploit Prevention process protection settings

*To open the **Processes protection settings** window:*

1. Expand the **Real-Time File Protection** node in the Application Console tree.
2. Select the **Exploit Prevention** node.
3. In the **Processes protection settings** section, click the **Process protection parameters** link.

   The **Processes protection settings** window opens.
4. Configure process protection settings for Exploit Prevention as required.

Configuring process memory protection settings

To add a process to the list of protected processes:

1. Open the **Exploit Prevention settings** window.
2. In the **Exploit prevention mode** block, configure the following settings:
   - **Prevent vulnerable processes exploit**.
     - **Terminate on exploit**.
     - **Notify only**.
3. In the **Preventing actions** block, configure the following settings:
   - **Notify about abused processes via Terminal Service**.
   - **Prevent vulnerable processes exploit even if Kaspersky Security Service is disabled**.
4. Click the **OK** button in the **Exploit Prevention settings** window.

Kaspersky Embedded Systems Security for Windows saves and applies the configured process memory protection settings.

Adding a process to the protection scope

The Exploit Prevention component protects several processes by default. You can uncheck the processes that you don't want to protect in the list of protected processes.

To add a process to the list of protected processes:

1. Open the **Processes protection settings** window.
2. To add a process to protect it from abuse and to reduce the potential impact of an exploit, perform the following actions:

   a. Click the **Browse** button.

   The standard Microsoft Windows **Open** window opens.

b. In the window that opens select a process you want to add to the list.

c. Click the **Open** button.

d. Click the **Add** button.

The process will be added to the list of protected processes.

3. Select a process in the list.

4. The current configuration is displayed on the **Processes protection settings** tab:

- **Process name**.
- **Is being executed**.
- **Exploit prevention techniques applied**.
- **Attack Surface Reduction settings**.

5. To modify the exploit prevention techniques that are applied to the process, select the **Deny modules for loading** tab.

6. Select one of the options for applying impact reduction techniques:

- **Apply all available exploit prevention techniques**.

  If this option is selected, the list cannot be edited. By default, all available techniques are applied to a process.

- **Apply listed exploit prevention techniques for the process**.

  If this option is selected, you can edit the list of impact reduction techniques applied:

  a. Select the check boxes next to the techniques that you want to apply to protect the selected process.

7. Configure settings for the Attack Surface Reduction technique:

- In the **Deny modules** field, enter the names of the modules whose launch from the protected process will be blocked.
- In the **Do not deny modules if launched in the Internet Zone** section, select the check boxes next to the options for which you want to allow modules to be launched:
  - **Internet**
  - **Local intranet**
  - **Trusted URL**
  - **Restricted sites**
  - **Computer**

  These settings only apply to Internet Explorer®.

8. Click the **Save** button.

The process is added to the task protection scope.

Managing Exploit Prevention via the Web Plug-in

In this section, learn how to navigate the Web Plug-in interface and configure the component settings on a protected device.

Configuring process memory protection settings

To configure Exploit Prevention settings for processes added to the list of protected processes, perform the following actions:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.
2. Click the policy name you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.
4. Select the **Real-Time Computer Protection** section.
5. Click **Settings** in the **Exploit Prevention** subsection.
6. Open the **Exploit Prevention settings** tab.
7. In the **Exploit prevention mode** block, configure the following settings:
   - Prevent vulnerable processes exploit.
     - Terminate on exploit.
     - Notify only.
8. In the **Preventing actions** block, configure the following settings:
   - Notify about abused processes via Terminal Service.
   - Prevent vulnerable processes exploit even if Kaspersky Security Service is disabled.
9. Click the **OK** button in the **Exploit Prevention** window.

Kaspersky Embedded Systems Security for Windows saves and applies the configured process memory protection settings.

Adding a process to the protection scope

To configure Exploit Prevention settings for processes added to the list of protected processes, perform the following actions:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Policies & profiles**.

2. Click the policy name you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.
4. Select the **Real-time computer protection** section.
5. Click **Settings** in the **Exploit Prevention** subsection.
6. Open the **Protected processes** tab.
7. Click the **Add** button.
8. The **Exploit prevention techniques** window opens.
9. Specify the process name.
10. Select one of the options for applying impact reduction techniques:
    - **Apply all available exploit prevention techniques**.

      If this option is selected, the list cannot be edited. By default, all available techniques are applied to a process.
    - **Apply selected exploit prevention techniques**

      If this option is selected, you can edit the list of impact reduction techniques applied:

      a. Select the check boxes next to the techniques that you want to apply to protect the selected process.

      b. Select or clear the **Apply Attack Surface Reduction technique** check box.
11. Configure settings for the Attack Surface Reduction technique:
    - Enter the names of the modules whose launch will be blocked from the protected process in the **Deny modules** field.
    - In the **Do not deny modules if launched in the Internet Zone** field, select the check boxes next to the options for which you want to allow modules to be launched:
      - **Internet**
      - **Local intranet**
      - **Trusted URL**
      - **Restricted URL**
      - **Computer**

      These settings only apply to Internet Explorer®.
12. Click the **OK** button.

The process is added to the task protection scope.

Exploit prevention techniques

Exploit prevention techniques

Exploit prevention technique	Description
Data Execution Prevention (DEP)	Data execution prevention blocks execution of arbitrary code in protected areas of memory.
Address Space Layout Randomization (ASLR)	Changes to the layout of data structures in the address space of the process.
Structured Exception Handler Overwrite Protection (SEHOP)	Replacement of exception records or replacement of the exception handler.
Null Page Allocation	Prevention of redirecting the null pointer.
LoadLibrary Network Call Check (Anti ROP)	Protection against loading DLLs from network paths.
Executable Stack (Anti ROP)	Blocking of unauthorized execution of areas of the stack.
Anti RET Check (Anti ROP)	Check that the CALL instruction is invoked safely.
Anti Stack Pivoting (Anti ROP)	Protection against relocation of the ESP stack pointer to an executable address.
Simple Export Address Table Access Monitor (EAT Access Monitor & EAT Access Monitor via Debug Register)	Protection of read access to the export address table for kernel32.dll, kernelbase.dll, and ntdll.dll
Heap Spray Allocation (Heapspray)	Protection against allocating memory to execute malicious code.
Execution Flow Simulation (Anti Return Oriented Programming)	Detection of potentially dangerous chains of instructions (potential ROP gadget) in the Windows API component.
IntervalProfile Calling Monitor (Ancillary Function Driver Protection (AFDP))	Protection against escalation of privileges through a vulnerability in the AFD driver (execution of arbitrary code in ring 0 through a QueryIntervalProfile call).
Attack Surface Reduction (ASR)	Blocking the start of vulnerable add-ins via the protected process.
Anti Process Hollowing (Hollowing)	Protection against creating and executing the malicious copies of trusted processes.
Anti AtomBombing (APC)	Global atom table exploit via Asynchronous Procedure Calls (APC).
Anti CreateRemoteThread (RThreadLocal)	Another process has created a thread in protected process.
Anti CreateRemoteThread (RThreadRemote)	Protected process has created a thread in another process.

Integrating with third-party systems

This section describes integration of Kaspersky Embedded Systems Security for Windows with third-party features and technologies.

Performance counters for System Monitor

This section contains information about performance counters for the Microsoft Windows System Monitor that are registered by Kaspersky Embedded Systems Security for Windows during installation.

About Kaspersky Embedded Systems Security for Windows performance counters

Performance Counters is a component of Kaspersky Embedded Systems Security for Windows that you can use to monitor application performance during execution of real-time computer protection tasks. You can identify bottlenecks when it is running with other applications and resource shortages. You can diagnose Kaspersky Embedded Systems Security for Windows crashes and identify undesirable settings.

You can view Kaspersky Embedded Systems Security for Windows performance counters by opening the **Performance** console in the **Administration** section of Windows Control Panel.

The following sections list definitions of counters, recommended intervals for taking readings, threshold values, and recommended Kaspersky Embedded Systems Security for Windows settings if the counter values exceed the thresholds.

Total number of requests denied

Total number of requests denied

Name	Total number of requests denied
Definition	Total number of object processing requests made by the file interception driver and not accepted by the application processes; counted from the time Kaspersky Embedded Systems Security for Windows was last started. The application skips objects for which processing requests are denied by Kaspersky Embedded Systems Security for Windows processes.
Purpose	This counter can help you detect: • Reduced Real-Time Computer Protection because Kaspersky Embedded Systems Security for Windows processes are overworked. • Interruption of Real-Time Computer Protection because of failures of file interception dispatchers.
Normal / threshold value	0 / 1
Recommended reading interval	1 hour.

Recommendations for configuration if value exceeds the threshold	The number of denied processing requests corresponds to the number of skipped objects. The following situations are possible depending on counter behavior: • The counter shows several requests denied over an extended period of time: all Kaspersky Embedded Systems Security for Windows processes were fully loaded, so Kaspersky Embedded Systems Security for Windows could not scan objects. To avoid skipping objects, increase the number of application processes for the Real-Time Computer Protection tasks. You can use such Kaspersky Embedded Systems Security for Windows settings as **Number of processes for real-time protection**. • The number of request denied significantly exceeds the critical threshold and is growing quickly: the file interception dispatcher has crashed. Kaspersky Embedded Systems Security for Windows is not scanning objects when they are accessed. Restart Kaspersky Embedded Systems Security for Windows.

Total number of requests skipped

Total number of requests skipped

Name	Total number of requests skipped
Definition	The total number of object processing requests made by the file interception driver that have been received by Kaspersky Embedded Systems Security for Windows and have not generated events indicating that processing is complete; this number is counted starting from the moment when the application was last started. If an object processing request is accepted by one of the work processes but does not send an event indicating that processing is complete, the driver will transfer the request to another process and the value of the **Total Number of Skipped Requests** counter will increase by 1. If the driver has gone through all of the work processes and none of them has accepted the processing request (all were busy) or has not sent an event indicating that processing is complete, Kaspersky Embedded Systems Security for Windows will skip the object, so the value of the **Total Number of Skipped Requests** counter will increase by 1.
Purpose	This counter enables you to detect drops in performance due to failures of file interception dispatchers.
Normal / threshold value	0 / 1
Recommended reading interval	1 hour.
Recommendations for configuration if value exceeds the threshold	If the counter is anything other than zero, this means that one or more file interception dispatcher streams have frozen and are down. The counter value corresponds to the number of streams currently down. If the scan speed is not satisfactory, restart Kaspersky Embedded Systems Security for Windows to restore the off-line streams.

Number of requests not processed because of lack of system resources

Number of requests not processed because of lack of system resources

Name	Number of requests not processed due to a lack of resources.
Definition	Total number of requests from the file interception driver which were not processed because of a lack of system resources (for example, RAM); counted from the time Kaspersky Embedded Systems Security for Windows was last started. Kaspersky Embedded Systems Security for Windows skips object processing requests that are not processed by the file interception driver.
Purpose	This counter can be used to detect and eliminate potentially lower quality in Real-Time Computer Protection that occurs because of low system resources.
Normal / threshold value	0 / 1
Recommended reading interval	1 hour.
Recommendations for configuration if value exceeds the threshold	If the counter value is anything other than zero, Kaspersky Embedded Systems Security for Windows work processes need more RAM to process requests. Active processes of other applications may be using all available RAM.

Number of requests sent to be processed

Number of requests sent to be processed

Name	Number of requests sent to be processed.
Definition	The number of objects waiting to be processed by work processes.
Purpose	This counter can be used to monitor the load on Kaspersky Embedded Systems Security for Windows work processes and the overall level of file activity on the protected device.
Normal / threshold value	The counter may vary depending on the level of file activity on the protected device.
Recommended reading interval	1 minute.
Recommendations for configuration if value exceeds the threshold	N/A

Average number of file interception dispatcher streams

Average number of file interception dispatcher streams

Name	Average number of file interception dispatcher streams.
Definition	The number of file interception dispatcher streams in one process and the average for all processes currently involved in the Real-Time Computer Protection tasks.
Purpose	This counter can be used to detect and eliminate a potential reduction in Real-Time Computer Protection due to a full load on Kaspersky Embedded Systems Security for Windows processes.
Normal / threshold value	Varies / 40

Recommended reading interval	1 minute.
Recommendations for configuration if value exceeds the threshold	Up to 60 file interception dispatcher streams can be created in each work process. If the counter approaches 60, there is a risk that none of the work processes will be able to process the next request in the queue from the file interception driver and Kaspersky Embedded Systems Security for Windows will skip the object. Increase the number of Kaspersky Embedded Systems Security for Windows processes for the Real-Time Computer Protection tasks. You can use such Kaspersky Embedded Systems Security for Windows settings as **Number of processes for real-time protection**.

Maximum number of file interception dispatcher streams

Maximum number of file interception dispatcher streams

Name	Maximum number of file interception dispatcher streams.
Definition	The number of file interception dispatcher streams in one process and the maximum for all processes currently involved in the Real-Time Computer Protection tasks.
Purpose	This counter enables you to detect and eliminate drops in performance because of uneven distribution of loads in running processes.
Normal / threshold value	Varies / 40
Recommended reading interval	1 minute.
Recommendations for configuration if value exceeds the threshold	If the value of this counter significantly and continuously exceeds the **Average number of file interception dispatcher streams** counter, Kaspersky Embedded Systems Security for Windows is distributing the load to running processes unevenly. Restart Kaspersky Embedded Systems Security for Windows.

Number of elements in the infected objects queue

Number of elements in the infected objects queue

Name	Number of elements in the infected objects queue.
Definition	Number of infected objects currently waiting to be processed (disinfected or deleted).
Purpose	This counter can help you detect: • Interruption of Real-Time Computer Protection due to potential failures of file interception dispatchers. • Overloading of processes due to uneven distribution of processor time among different work processes and Kaspersky Embedded Systems Security for Windows. • Virus outbreaks.
Normal / threshold	This value may be something other than zero while Kaspersky Embedded Systems

value	Security for Windows is processing infected or probably infected objects but will return to zero after processing is finished / The value remains non-zero for an extended period of time.
Recommended reading interval	1 minute.
Recommendations for configuration if value exceeds the threshold	If the value of the counter does not return to zero for an extended period of time: • Kaspersky Embedded Systems Security for Windows is not processing objects (the file interception dispatcher may have crashed). Restart Kaspersky Embedded Systems Security for Windows. • There may be insufficient processor time to process the objects. Make sure Kaspersky Embedded Systems Security for Windows receives additional processor time (by reducing other applications' load on the protected device, for example). • There has been a virus outbreak. A large number of infected or probably infected objects in the Real-Time File Protection task is also a sign of a virus outbreak. You can view information about the number of detected objects in the task statistics or task logs.

Number of objects processed per second

Number of objects processed per second

Name	Number of objects processed per second.
Definition	Number of objects processed divided by the amount of time that it took to process those objects (calculated over equal time intervals).
Purpose	This counter reflects the speed of object processing; it can be used to detect and eliminate low points in protected device performance that occur because of insufficient processor time being allotted to Kaspersky Embedded Systems Security for Windows processes or errors in Kaspersky Embedded Systems Security for Windows operation.
Normal / threshold value	Varies / No.
Recommended reading interval	1 minute.
Recommendations for configuration if value exceeds the threshold	The values of this counter depend on the values set in Kaspersky Embedded Systems Security for Windows settings and the load on the protected device from other applications' processes. Observe the average counter value over an extended period of time. If the average counter value decreases, one of the following situations is possible: • Kaspersky Embedded Systems Security for Windows processes do not have enough processor time to process the objects. Make sure Kaspersky Embedded Systems Security for Windows receives additional processor time (by reducing other applications' load on the protected device, for example). • Kaspersky Embedded Systems Security for Windows has experienced an error (several streams are idle). Restart Kaspersky Embedded Systems Security for Windows.

Kaspersky Embedded Systems Security for Windows SNMP counters and traps

This section contains information about Kaspersky Embedded Systems Security for Windows counters and traps.

About Kaspersky Embedded Systems Security for Windows SNMP counters and traps

If you included SNMP Counters and Traps in the set of anti-virus components to be installed, you can view Kaspersky Embedded Systems Security for Windows counters and traps using Simple Network Management Protocol (SNMP).

To view Kaspersky Embedded Systems Security for Windows counters and traps from the administrator's workstation, start SNMP Service on the protected device and start SNMP and SNMP Trap Services on the administrator's workstation.

Kaspersky Embedded Systems Security for Windows SNMP counters

This section contains tables with a description of the settings for Kaspersky Embedded Systems Security for Windows SNMP counters.

Performance counters

Performance counters

Counter	Definition
currentRequestsAmount	Number of requests sent to be processed
currentInfectedQueueLength	Number of elements in the infected objects queue
currentObjectProcessingRate	Number of objects processed per second
currentWorkProcessesNumber	Current number of work processes used by Kaspersky Embedded Systems Security for Windows

Quarantine counters

Quarantine counters

Counter	Definition
totalObjects	Number of objects currently in Quarantine
totalSuspiciousObjects	Number of probably infected objects currently in Quarantine
currentStorageSize	Total amount of data in Quarantine (MB)

Backup counter

Backup counter

Counter	Definition
currentBackupStorageSize	Total amount of data in Backup (MB)

General counters

General counters

Counter	Definition
lastCriticalAreasScanAge	The period since the last complete scan of the protected device's critical areas (time elapsed in seconds since the last Critical Areas Scan task was completed).
licenseExpirationDate	License expiration date. If an active and additional key have been added, the date of expiry of the license associated with the additional key is displayed.
currentApplicationUptime	The amount of time that Kaspersky Embedded Systems Security for Windows has been running since it was last started, in hundredths of seconds.

Update counter

Update counter

Counter	Definition
avBasesAge	"Age" of databases (time elapsed in hundredths of seconds since the creation date of the latest installed database updates).

Real-Time File Protection counters

Real-Time File Protection counters

Counter	Definition
totalObjectsProcessed	Total number of objects scanned since the time the last Real-Time File Protection task was run
totalInfectedObjectsFound	Total number of infected and other objects detected since the time the last Real-Time File Protection task was run
totalSuspiciousObjectsFound	Total number of probably infected objects detected since the time the last Real-Time File Protection task was run
totalVirusesFound	Total number of objects detected since the time the Real-Time File Protection task was last run
totalObjectsQuarantined	Total number of infected, probably infected and other objects which were placed into Quarantine by Kaspersky Embedded Systems Security for

	Windows; calculated from the time the Real-Time File Protection task was last started
totalObjectsNotQuarantined	Total number of infected or probably infected objects Kaspersky Embedded Systems Security for Windows attempted to quarantine but was unable to; calculated from the time the Real-Time File Protection task was last started
totalObjectsDisinfected	Total number of infected objects which were disinfected by Kaspersky Embedded Systems Security for Windows; calculated from the time the Real-Time File Protection task was last started
totalObjectsNotDisinfected	Total number of infected and other objects which Kaspersky Embedded Systems Security for Windows attempted to disinfect but was unable to; calculated from the time Real-Time File Protection task was last started
totalObjectsDeleted	Total number of infected, probably infected and other objects which were deleted by Kaspersky Embedded Systems Security for Windows; calculated from the time the Real-Time File Protection task was last started
totalObjectsNotDeleted	Total number of infected, probably infected and other objects which Kaspersky Embedded Systems Security for Windows attempted to delete but was unable to; calculated from the time Real-Time File Protection task was last started
totalObjectsBackedUp	Total number of infected objects and other which were placed into Backup by Kaspersky Embedded Systems Security for Windows; calculated from the time the Real-Time File Protection task was last started
totalObjectsNotBackedUp	Total number of infected objects and other which Kaspersky Embedded Systems Security for Windows attempted to place into Backup but was unable to; calculated from the time Real-Time File Protection task was last started

Kaspersky Embedded Systems Security for Windows SNMP traps and their options

The SNMP traps options in Kaspersky Embedded Systems Security for Windows are summarized as follows:

- eventThreatDetected: an object has been detected.

  The trap has the following options:

  - eventDateAndTime
  - eventSeverity
  - computerName
  - userName
  - objectName
  - threatName
  - detectType

- detectCertainty

- eventBackupStorageSizeExceeds: maximum Backup size exceeded. The total amount of data in Backup exceeds the value specified by **Maximum Backup size (MB)**. Kaspersky Embedded Systems Security for Windows continues to back up infected objects.

  The trap has the following options:

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventThresholdBackupStorageSizeExceeds: Backup free space threshold reached. The amount of free space in Backup is less than or equal to the value specified by **Threshold value for space available (MB)**. Kaspersky Embedded Systems Security for Windows continues to back up infected objects.

  The trap has the following options:

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventQuarantineStorageSizeExceeds: maximum Quarantine size exceeded. The total size of data in Quarantine has exceeded the value specified by the **Maximum Quarantine size (MB)**. Kaspersky Embedded Systems Security for Windows continues to quarantine probably infected objects.

  The trap has the following options:

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventThresholdQuarantineStorageSizeExceeds: Quarantine free space threshold reached. The amount of free size in Quarantine assigned by the **Threshold value for space available (MB)** is equal to or less than the specified value. Kaspersky Embedded Systems Security for Windows continues to back up infected objects.

  The trap has the following options:

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventObjectNotQuarantined: Quarantine error.

  The trap has the following options:

  - eventSeverity
  - eventDateAndTime
  - eventSource

- userName
- computerName
- objectName
- storageObjectNotAddedEventReason

- eventObjectNotBackuped: Error while saving an object copy in Backup.

  The trap has the following options:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - objectName
  - userName
  - computerName
  - storageObjectNotAddedEventReason

- eventQuarantineInternalError: Quarantine internal error.

  The trap has the following options:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason

- eventBackupInternalError: Backup error.

  The trap has the following options:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason

- eventAVBasesOutdated: Anti-virus database is out of date. Number of days since the last time the Database Update task (local task, or group task, or task for sets of protected devices) was run.

  The trap has the following options:

  - eventSeverity
  - eventDateAndTime

- eventSource
- days

- eventAVBasesTotallyOutdated: Anti-virus database is obsolete. Number of days since the last time the Database Update task (local task, or group task, or task for sets of protected devices) was run.

  The trap has the following options:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventApplicationStarted: Kaspersky Embedded Systems Security for Windows is running.

  The trap has the following options:

  - eventSeverity
  - eventDateAndTime
  - eventSource

- eventApplicationShutdown: Kaspersky Embedded Systems Security for Windows is stopped.

  The trap has the following options:

  - eventSeverity
  - eventDateAndTime
  - eventSource

- eventCriticalAreasScanWasntPerformForALongTime: Critical areas have not been scanned for a long time. Number of days since the last time the Critical Areas Scan task completed.

  The trap has the following options:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventLicenseHasExpired: License has expired.

  The trap has the following options:

  - eventSeverity
  - eventDateAndTime
  - eventSource

- eventLicenseExpiresSoon: License expires soon. Calculated as the number of days until the expiration date for the license.

  The trap has the following options:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventTaskInternalError: Task completion error.

  The trap has the following options:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - errorCode
  - knowledgeBaseId
  - taskName

- eventUpdateError: Error while running the update task.

  The trap has the following options:

  - eventSeverity
  - eventDateAndTime
  - taskName
  - updaterErrorEventReason

Kaspersky Embedded Systems Security for Windows SNMP traps options descriptions and possible values

Descriptions of the traps options and their possible values are given below:

- eventDateAndTime: event date and time.
- eventSeverity: importance level.

  The option can take the following values:

  - critical (1) – critical
  - warning (2) – warning

- info (3) – informational

- userName: user name (for example, the name of a user that attempted to access an infected file).

- computerName: protected device name (for example, the name of a protected device from which a user attempted to access an infected file).

- eventSource: functional component that generated the event.

  The option can take the following values:

  - unknown (0) – functional component not known
  - quarantine (1) – Quarantine
  - backup (2) – Backup
  - reporting (3) – task logs
  - updates (4) – Update
  - realTimeProtection (5) – Real-Time File Protection
  - onDemandScanning (6) – On-Demand Scan
  - product (7) – event related to operation of Kaspersky Embedded Systems Security for Windows as a whole rather than operation of individual components
  - systemAudit (8) – system audit log

- eventReason: event trigger: what triggered the event.

  The option can take the following values:

  - reasonUnknown (0) – reason is unknown.
  - reasonInvalidSettings (1) – only for Backup and Quarantine events. Displayed if the Quarantine or Backup folder is unavailable (insufficient access permissions or an invalid folder is specified in the Quarantine settings, for example, a network path is specified). In this case, Kaspersky Embedded Systems Security for Windows will use the default Backup or Quarantine folder.

- objectName: an object name (for example, the name of the file where the virus was detected).

- threatName: The name of the object according to the Virus Encyclopedia classification. This name is included in the full name that Kaspersky Embedded Systems Security for Windows returns on detecting an object. You can view the full name of a detected object in the task log.

- detectType: type of object detected.

  The option can take the following values:

  - undefined (0) – undefined
  - virware – classic viruses and network worms
  - trojware – Trojans
  - malware – other malicious applications

- adware – advertising software
- pornware – pornographic software
- riskware – legitimate applications that may be used by intruders to damage the user's device or personal data

- detectCertainty: certainty level for threat detection.

  The option can take the following values:

  - Suspicion (probably infected) – Kaspersky Embedded Systems Security for Windows has detected a partial match between a section of object code and a known section of malicious code.
  - Sure (infected) – Kaspersky Embedded Systems Security for Windows has detected a complete match between a section of code in the object and a known section of malicious code.

- days: number of days (for example, the number of days until the license expiration date).
- errorCode: an error code.
- knowledgeBaseId: address of a knowledge base article (for example, address of an article that explains a particular error).
- taskName: a task name.
- updaterErrorEventReason: the reason for the update error.

  The option can take the following values:

  - reasonUnknown(0) – reason is unknown.
  - reasonAccessDenied – access denied.
  - reasonUrlsExhausted – the list of update sources has been exhausted.
  - reasonInvalidConfig – invalid configuration file.
  - reasonInvalidSignature – invalid signature.
  - reasonCantCreateFolder – folder cannot be created.
  - reasonFileOperError – file error.
  - reasonDataCorrupted – object is corrupted.
  - reasonConnectionReset – connection reset.
  - reasonTimeOut – connection timeout exceeded.
  - reasonProxyAuthError – proxy authentication error.
  - reasonServerAuthError – server authentication error.
  - reasonHostNotFound – device not found.
  - reasonServerBusy – server unavailable.

- reasonConnectionError – connection error.
- reasonModuleNotFound – object not found.
- reasonBlstCheckFailed(16) – error while checking the key denylist. It is possible that database updates were being published at the time of the update; please repeat the update in a few minutes.

- storageObjectNotAddedEventReason: the reason why the object was not put in Backup or Quarantine.

  The option can take the following values:

  - reasonUnknown (0) – reason is unknown.
  - reasonStorageInternalError – database error; Kaspersky Embedded Systems Security for Windows must be restored.
  - reasonStorageReadOnly – database is read-only; Kaspersky Embedded Systems Security for Windows must be restored.
  - reasonStorageIOError – input-output error: a) Kaspersky Embedded Systems Security for Windows is corrupted and needs to be restored; b) the disk where Kaspersky Embedded Systems Security for Windows files are stored is corrupted.
  - reasonStorageCorrupted – storage is corrupted; Kaspersky Embedded Systems Security for Windows must be restored.
  - reasonStorageFull – database is full; free disk space is required.
  - reasonStorageOpenError – database file could not be opened; Kaspersky Embedded Systems Security for Windows must be restored.
  - reasonStorageOSFeatureError – some operating system features do not correspond to Kaspersky Embedded Systems Security for Windows requirements.
  - reasonObjectNotFound – object being placed in Quarantine does not exist on the disk.
  - reasonObjectAccessError – insufficient permissions to use Backup API: the account being used to perform the operation does not have Backup Operator permissions.
  - reasonDiskOutOfSpace – not enough space on the disk.

Integrating with WMI

Kaspersky Embedded Systems Security for Windows supports integration with Windows Management Instrumentation (WMI): you can use client systems that use WMI to receive data via the Web-Based Enterprise Management (WBEM) standard in order to receive information about the status of Kaspersky Embedded Systems Security for Windows and its components.

When Kaspersky Embedded Systems Security for Windows is installed, it registers a proprietary module on the system to create a Kaspersky Embedded Systems Security for Windows namespace on the protected device. A Kaspersky Embedded Systems Security for Windows namespace lets you work with Kaspersky Embedded Systems Security for Windows classes and instances and their properties.

The values of some instance properties depend on task types.

A *non-periodic task* is an application task that is not time-limited and can either be constantly running or stopped. Such tasks have no execution progress. The task results are logged continuously while the task is running as single events (for example, detection of an infected object by any Real-Time Computer Protection tasks). This type of tasks is managed via Kaspersky Security Center policies.

A *periodic task* is an application task that is time-limited and has execution progress displayed as a percentage. The task results are generated when the task is complete and are represented as a single item or changed application state (for example, completed application database update, generated configuration files for rule generation tasks). Several periodic tasks of the same type can run on a single protected device simultaneously (e.g. three On-Demand scan tasks with different scan scopes). Periodic tasks can be managed via Kaspersky Security Center as group tasks.

If you use tools to generate WMI namespace queries and receive dynamic data from WMI namespaces on your corporate network, you will be able to receive information about the current application state (see the table below).

Information about the application state

Instance property	Description	Values
ProductName	Name of the installed application.	Full name of application without version number.
ProductVersion	Full version of the installed application.	Full application version number, including the build number.
InstalledPatches	Set of display names for installed patches.	List of critical fixes installed for the application.
IsLicenseInstalled	Application activation status.	Status of the key used to activate the application. Possible values: • False - A license key has not been added to the application. • True - A license key has been added to the application.
LicenseDaysLeft	Shows how many days are left before a current license expiration.	Number of days remaining before expiration of the current license. Possible non-positive values: • 0 - License has expired. • -1 - Unable to get information on the current key or the specified key cannot be used to activate the application (for example, it is blocked based on key denylist).
AVBasesDatetime	Timestamp for the current anti-virus database version.	Date and time of the creation of the anti-virus databases currently in use. If the installed application does not use anti-virus databases, then the field has the value “Not installed”.
IsExploitPreventionEnabled	Status of the Exploit Prevention component.	Status of the Exploit Prevention component. Possible values:

		• True - The Exploit Prevention component is enabled and providing protection. • False - The Exploit Prevention component is not providing protection. For example: disabled, not installed, the License Agreement has been violated.
ProtectionTasksRunning	Set of protection tasks that are currently running.	List of protection, control, and monitoring tasks currently running. This field should account for all running non-periodic tasks. If no non-periodic task is running, the field has the value "None".
IsAppControlRunning	Status of the Applications Launch Control task.	Status of the Applications Launch Control task. • True - The Applications Launch Control task is currently running. • False - The Applications Launch Control is not currently running or the Applications Launch Control component is not installed.
AppControlMode	Applications Launch Control task mode.	Describes the current status of the Applications Launch Control component, and describes the selected mode for the corresponding task. Possible values: • Active - **Active** mode is selected in the task settings. • Statistics Only - **Statistics only** mode is selected in the task settings. • Not installed - The Applications Launch Control component is not installed.
AppControlRulesNumber	Total number of applications launch control rules.	The number of rules currently specified in the Applications Launch Control task settings.
AppControlLastBlocking	The timestamp for the last application launch blocking by the Applications Launch Control task in any mode.	Date and time when the Applications Launch Control component last blocked the launch of an application. This field includes all blocked applications, regardless of the task mode. If no instances of blocked application launches are registered at the time the WMI query is processed, the field is assigned the value "None".
PeriodicTasksRunning	Set of periodic tasks that are currently running.	List of On-Demand Scan, Update, and inventory-taking tasks currently running. This field should include all running periodic tasks. If no periodic tasks are currently running, then the field has the value "None".
ConnectionState	Status of the connection	Information about the status of the

	between the WMI Provider component and the Kaspersky Security Service (KAVFS).	connection between the WMI Provider component and the Kaspersky Security Service. Possible values: • Success - The connection was successfully established: the WMI client can receive the application status. • Failed. Error Code: <code> - The connection could not be established due to an error with the specified code.

This data represents instance properties KasperskySecurity_ProductInfo.ProductName=Kaspersky Embedded Systems Security for Windows, where:

- KasperskySecurity_ProductInfo is the name of the Kaspersky Embedded Systems Security for Windows class
- .ProductName=Kaspersky Embedded Systems Security for Windows are the Kaspersky Embedded Systems Security for Windows key properties

The instance is created in the ROOT\Kaspersky\Security namespace.

Working with Kaspersky Embedded Systems Security for Windows from the command line

This section describes working with Kaspersky Embedded Systems Security for Windows from the command line.

Commands

You can perform basic Kaspersky Embedded Systems Security for Windows management commands from the command line of the protected device using the Command Line utility component, which is included in the Kaspersky Embedded Systems Security for Windows software components group.

You can use commands to manage only those functions accessible to you based on the permissions assigned to you in Kaspersky Embedded Systems Security for Windows.

Certain Kaspersky Embedded Systems Security for Windows commands are executed in the following modes:

- Synchronous mode: control returns to the Console only after the command is complete.
- Asynchronous mode: control returns to the Console immediately after the command is started.

To interrupt a command being executed in synchronous mode,

press the **Ctrl+C** keyboard shortcut.

Follow these rules when entering Kaspersky Embedded Systems Security for Windows commands:

- Enter modifiers and commands using upper and lower case.
- Separate modifiers with a space.
- If the path of a file/folder specified as a value includes a space, enclose the path in quotes, for example: `"C:\TEST\test cpp.exe"`.
- If necessary, you can use wildcards in the filename or path, for example: `"C:\Temp\Temp*\"`, `"C:\Temp\Temp???.doc"`, `"C:\Temp\Temp*.doc"`.

You can use the command line to perform every operation required for management and administration of Kaspersky Embedded Systems Security for Windows (see the table below).

Kaspersky Embedded Systems Security for Windows commands

Command	Description
KAVSHELL APPCONTROL	Update the rule list according to the selected import rule.
KAVSHELL APPCONTROL /CONFIG	Set the operating mode of the Applications Launch Control task
KAVSHELL APPCONTROL /GENERATE	Start the Rule Generator for Applications Launch Control task.
KAVSHELL VACUUM	Defragment Kaspersky Embedded Systems Security for Windows log files.

KAVSHELL PASSWORD	Manage password protection settings.
KAVSHELL HELP	Display Kaspersky Embedded Systems Security for Windows command help.
KAVSHELL START	Start the Kaspersky Security Service.
KAVSHELL STOP	Stop the Kaspersky Security Service.
KAVSHELL SCAN	Create and start a temporary On-Demand Scan task with the scan scope and security settings specified by the command-line options.
KAVSHELL SCANCRITICAL	Start the Critical Areas Scan local system task.
KAVSHELL TASK	Starts, pauses, resumes, or stops the specified task asynchronously. Returns the current task status / task statistics.
KAVSHELL RTP	Start or stop all Real-Time Computer Protection tasks.
KAVSHELL UPDATE	Start the Database Update task with the settings specified by the command-line options.
KAVSHELL ROLLBACK	Roll back the databases to the previous version.
KAVSHELL LICENSE	Add or delete the keys. Display information about the added keys.
KAVSHELL TRACE	Enable or disable tracing. Manage tracing settings.
KAVSHELL DUMP	Enable or disable creation of dump files when Kaspersky Embedded Systems Security for Windows processes terminate abnormally.
KAVSHELL IMPORT	Import general Kaspersky Embedded Systems Security for Windows settings, functions, and tasks from a configuration file.
KAVSHELL EXPORT	Export all Kaspersky Embedded Systems Security for Windows settings and existing tasks to a configuration file.
KAVSHELL DEVCONTROL	Add to the list of generated device control rules according to selected method.

Displaying command help for Kaspersky Embedded Systems Security for Windows. KAVSHELL HELP

To view the list of all Kaspersky Embedded Systems Security for Windows commands, run one of the following commands:

```
KAVSHELL

KAVSHELL HELP

KAVSHELL /?
```

To view a description of a command and its syntax, run one of the following commands:

```
KAVSHELL HELP <command>
```

```
KAVSHELL <command> /?
```

KAVSHELL HELP examples

To view detailed information about the KAVSHELL SCAN command, execute the following command:

```
KAVSHELL HELP SCAN
```

Starting and stopping the Kaspersky Security Service: KAVSHELL START, KAVSHELL STOP

To run the Kaspersky Security Service, execute the following command:

```
KAVSHELL START
```

By default, when the Kaspersky Security Service is started, Real-Time File Protection and Scan at Operating System Startup, as well as other tasks scheduled to start **At application launch**, will be started.

To stop the Kaspersky Security Service, execute the following command:

```
KAVSHELL STOP
```

A password might be required to execute the command. To enter the current password, use `[/pwd: <password>]`.

Scanning a specified scope: KAVSHELL SCAN

To start a task to scan specific areas of the protected device, use `KAVSHELL SCAN`. The command-line options specify the scan scope and security settings of the selected node.

An On-Demand Scan task started using the `KAVSHELL SCAN` command is a temporary task. It is displayed in the Application Console only while being executed (you cannot view its task settings in the Application Console). However, a task log is generated and displayed in the **Task logs** in the Application Console.

When specifying paths in scan tasks for specific areas, you can use environment variables. If you use a user environment variable, execute the `KAVSHELL SCAN` command as the corresponding user.

The `KAVSHELL SCAN` command is executed in synchronous mode.

To start an existing On-Demand Scan task from the command line, use the KAVSHELL TASK command.

KAVSHELL SCAN command syntax

```
KAVSHELL SCAN <scan scope> [/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP] [/L:<
path to file with the list of scan scopes >] [/F<A|C|E>] [/NEWONLY] [/AI:
<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>] [/AS:<QUARANTINE|DELETE|REPORT|AUTO>]
[/DISINFECT|/DELETE] [/E:<ABMSPO>] [/EM:<"masks">] [/ES:<size>] [/ET:<number of seconds>]
[/TZOFF] [/OF:<SKIP|RESIDENT|SCAN[=<days>] [NORECALL]>] [/NOICHECKER][/NOISWIFT]
[/ANALYZERLEVEL][/NOCHECKMSSIGN][/W:<path to task log file>] [/ANSI] [/ALIAS:<task
alias>]
```

The KAVSHELL SCAN command has both mandatory and optional parameters/options (see the table below).

KAVSHELL SCAN command example

```
KAVSHELL SCAN Folder56 D:\Folder1\Folder2\Folder3\ C:\Folder1\ C:\Folder2\3.exe
"\\another server\Shared\" F:\123\*.fgb /SHARED /AI:DISINFDEL /AS:QUARANTINE /FA /E:ABM
/EM:"*.xtx;*.fff;*.ggg;*.bbb;*.info" /NOICHECKER /ANALYZERLEVEL:1 /NOISWIFT /W:log.log

KAVSHELL SCAN /L:scan_objects.lst /W:c:\log.log
```

KAVSHELL SCAN command-line parameters/options

Parameter/option	Description
Scan scope. The setting is mandatory.	
<files> <folders> <network path>	Specifies the scan scope - list of files, folders, network paths and predefined areas. Specify network paths in Universal Naming Convention (UNC) format. In the following example, Folder4 is specified without the path to it. This means that it is located in the folder from which you run the KAVSHELL command. KAVSHELL SCAN Folder4 If the name of the object to be scanned has spaces, it must be wrapped in quotation marks. If a folder is specified, Kaspersky Embedded Systems Security for Windows will also scan all its subfolders. The symbols * or ? can be used to scan a group of files.
/MEMORY	Scan objects in RAM
/SHARED	Scan shared folders on the protected device
/STARTUP	Scan autorun objects
/REMDRIVES	Scan removable drives
/FIXDRIVES	Scan hard drives
/MYCOMP	Scan all areas of the protected device
/L:<path to file with a list of scan scopes>	Full path to file with a list of scan scopes. Use line breaks to separate the scan scopes in the file. You can specify predefined scan areas as shown in the following example of the content of a file with a list of scan scopes: C:\ D:\Docs*.doc E:\My Documents /STARTUP /SHARED

Scan objects (File types). If you do not specify this option, Kaspersky Embedded Systems Security for Windows will scan objects by their format.	
/FA	Scan all objects
/FC	Scan objects by format (default). Kaspersky Embedded Systems Security for Windows scans only objects whose formats are included in the list of formats of infectable objects.
/FE	Scan objects by extension. Kaspersky Embedded Systems Security for Windows scans only objects with extensions included into the list of extensions of infectable objects.
/NEWONLY	Scan only new and modified files. If you do not specify this option, Kaspersky Embedded Systems Security for Windows will scan all objects.
Action to perform on infected and other objects. If you do not specify values for this modifier, Kaspersky Embedded Systems Security for Windows will perform the **Skip** action.	
DISINFECT	Disinfect, skip if disinfection is not possible The DISINFECT and DELETE options are preserved in the current version Kaspersky Embedded Systems Security for Windows in order to ensure compatibility with previous versions. These options can be used instead of the /AI and /AS options. In this case, Kaspersky Embedded Systems Security for Windows will not process probably infected objects.
DISINFDEL	Disinfect, delete if disinfection is not possible
DELETE	Delete The DISINFECT and DELETE options are preserved in the current version Kaspersky Embedded Systems Security for Windows in order to ensure compatibility with previous versions. These options can be used instead of the /AI and /AS options. In this case, Kaspersky Embedded Systems Security for Windows will not process probably infected objects.
REPORT	Send report (default)
AUTO	Perform recommended action
Action to perform on probably infected objects. If you do not specify this option, Kaspersky Embedded Systems Security for Windows will perform the **Skip** action.	
QUARANTINE	Quarantine
DELETE	Delete
REPORT	Send report (default)
AUTO	Perform recommended action
Exclusions	
/E:ABMSPO	Exclude the following types of compound objects: A – archives (scan SFX archives only) B – email databases M – plain mail S – archives and SFX-archives P – packed objects O – embedded OLE objects
/EM:<"masks">	Exclude files by mask

	You can specify several masks, for example: `EM:"*.txt; *.png; C\Videos\*.avi"`.
/ET:<number of seconds>	Stop processing an object if it takes longer than the number of seconds specified by <number of seconds>. By default, there is no time restriction.
/ES:<size>	Do not scan compound objects larger than the size (in MB) specified by the value <size>. By default, Kaspersky Embedded Systems Security for Windows scans objects of all sizes.
/TZOFF	Disable Trusted Zone exclusions
Advanced settings (Options)	
/NOICHECKER	Disable the use of iChecker (enabled by default)
/NOISWIFT	Disable the use of iSwift (enabled by default)
/ANALYZERLEVEL: <heuristic analysis level>	Enable Heuristic Analyzer, configure analysis level. The following heuristic analysis levels are available: 1 – light 2 – medium 3 – deep If you omit this option, Kaspersky Embedded Systems Security for Windows will not use Heuristic Analyzer.
/ALIAS:<task alias>	Assigns a temporary name to an On-Demand Scan task, allowing you to reference it while it runs, for example, in order to view its statistics using the TASK command. The task alias must be unique among the task aliases of all Kaspersky Embedded Systems Security for Windows components. If this option is not specified, a temporary name in the form of scan_<kavshell_pid> is assigned, for example, scan_1234. In the Application Console, the task is assigned the name "Scan objects <date and time>", for example, Scan objects 8/16/2007 5:13:14 PM.
Task log settings (Report settings)	
/W:<path to task log file>	If this parameter is specified, Kaspersky Embedded Systems Security for Windows will save the task log file using the name specified by the parameter value. The log file contains task execution statistics, the time when the task was started and completed (stopped), and information about events that occurred during the task. The log is used to register events defined by the task log settings and the Kaspersky Embedded Systems Security for Windows event log settings in Event Viewer. You can specify either the absolute or relative path to the log file. If you specify only a filename without a path, the log file will be created in the current folder. Restarting the command with the same log settings will overwrite the existing log file. The log file can be viewed while a task is running. The log appears in the Task logs node of the Application Console. If Kaspersky Embedded Systems Security for Windows fails to create the log file, it will display an error message but will still execute the command.
/ANSI	This option uses ANSI encoding to record events to the task log. The ANSI option will not be applied if the W parameter is not specified. If the ANSI option is not specified, UNICODE is used to generate the task log.

Starting the Critical Areas Scan task: KAVSHELL SCANCRITICAL

Use the `KAVSHELL SCANCRITICAL` command to start the Critical Areas Scan task with the settings defined in the Application Console.

KAVSHELL SCANCRITICAL command syntax

```
KAVSHELL SCANCRITICAL [/W:<path to task log file>]
```

KAVSHELL SCANCRITICAL command examples

To run the Critical Areas Scan task and save a task log named scancritical.log in the current folder, execute the following command:

```
KAVSHELL SCANCRITICAL /W:scancritical.log
```

You can use the /W parameter to configure the location of the task log (see the table below).

Syntax of the `/W` parameter for the `KAVSHELL SCANCRITICAL` command

Parameter/option	Description
/W:<path to task log file>	If this parameter is specified, Kaspersky Embedded Systems Security for Windows will save the task log file using the name specified by the parameter value. The log file contains task execution statistics, the time when the task was started and completed (stopped), and information about events that occurred during the task. The log is used to register events defined by the task log settings and the Kaspersky Embedded Systems Security for Windows event log settings in Event Viewer. You can specify either the absolute or relative path to the log file. If you specify only a filename without a path, the log file will be created in the current folder. Restarting the command with the same log settings will overwrite the existing log file. The log file can be viewed while a task is running. The log appears in the **Task logs** node of the Application Console. If Kaspersky Embedded Systems Security for Windows fails to create the log file, it will display an error message but will still execute the command.

Managing tasks asynchronously: KAVSHELL TASK

You can use the `KAVSHELL TASK` command to manage the specified task: run, pause, resume and stop the task and view the current task status and statistics. The command is performed in asynchronous mode.

A password might be required to execute the command. To enter the current password, use `[/pwd:<password>]`.

KAVSHELL TASK command syntax

```
KAVSHELL TASK [<task name alias> </START | /STOP | /PAUSE | /RESUME | /STATE |
/STATISTICS >]
```

KAVSHELL TASK command example

```
KAVSHELL TASK

KAVSHELL TASK on-access /START

KAVSHELL TASK user-task_1 /STOP

KAVSHELL TASK scan-computer /STATE

KAVSHELL TASK network-attack-blocker /START
```

The `KAVSHELL TASK` command can run without parameters/options or with one or more parameters/options (see the table below).

KAVSHELL TASK command-line parameters/options

Parameter/option	Description
No parameters	Return the list of all existing Kaspersky Embedded Systems Security for Windows tasks. The list includes the following fields: task alias, task category (system or custom) and current task status.
<task alias>	Instead of the task name, in the SCAN TASK command, use its task alias, an additional abbreviated name that Kaspersky Embedded Systems Security for Windows assigns to tasks. To view Kaspersky Embedded Systems Security for Windows task aliases, enter the KAVSHELL TASK command without any parameters.
/START	Start the specified task in asynchronous mode.
/STOP	Stop the specified task.
/PAUSE	Pause the specified task.
/RESUME	Resume the specified task in asynchronous mode.
/STATE	Return the current task status (for example, *Running*, *Completed*, *Paused*, *Stopped*, *Failed*, *Starting*, *Resuming*)
/STATISTICS	Retrieve task statistics - Information about the number of objects processed from the time the task started

Note that not all Kaspersky Embedded Systems Security for Windows tasks fully support /PAUSE, /RESUME and /STATE keys.

Return codes for the KAVSHELL TASK command.

Removing the PPL attribute: KAVSHELL CONFIG

The `KAVSHELL CONFIG` command lets you remove the PPL (Protected Process Light) attribute for the Kaspersky Security Service using the ELAM driver installed during installation of the application.

KAVSHELL CONFIG command syntax

```
KAVSHELL CONFIG /PPL:<OFF>
```

KAVSHELL CONFIG command-line parameters/options

Parameter/option	Description
/PPL:OFF	Remove the PPL attribute for the Kaspersky Security Service.

Starting and stopping Real-Time Computer Protection tasks. KAVSHELL RTP

You can use the `KAVSHELL RTP` command to start or stop all the Real-Time Computer Protection tasks.

A password might be required to execute the command. To enter the current password, use `[/pwd:<password>]`.

KAVSHELL RTP command syntax

```
KAVSHELL RTP {/START | /STOP}
```

KAVSHELL RTP command example

To start all the Real-Time Computer Protection tasks, execute the following command:

```
KAVSHELL RTP /START
```

The `KAVSHELL RTP` command must include one of two options (see the table below).

KAVSHELL RTP command-line options

Parameter/option	Description
/START	Start all the Real-Time Computer Protection tasks: Real-Time File Protection and KSN Usage.
/STOP	Stop all the Real-Time Computer Protection tasks.

Managing the Applications Launch Control task: KAVSHELL APPCONTROL /CONFIG

You can use the `KAVSHELL APPCONTROL /CONFIG` command to configure the mode in which the Applications Launch Control task runs and monitors the loading of DLL modules.

KAVSHELL APPCONTROL /CONFIG command syntax

```
/config /mode:<applyrules|statistics> [/dll:<no|yes>] | /config /savetofile:<full path to XML file>
```

KAVSHELL APPCONTROL /CONFIG command examples

*To run the Applications Launch Control task in **Active** mode without monitoring DLL loading save the task settings upon completion, run the following command:*

```
KAVSHELL APPCONTROL /CONFIG /mode:applyrules /dll:<no>
/savetofile:c:\appcontrol\config.xml
```

You can configure Applications Launch Control task settings using the command-line parameters (see the table below).

`KAVSHELL APPCONTROL /CONFIG` command-line parameters/options

Parameter/option	Description
`/mode:<applyrules|statistics>`	Applications Launch Control task mode. You can select one of the following modes: • `applyrules` - Apply Applications Launch Control rules; • `statistics` - Only generate statistics.
`/dll:<no|yes>`	Enable or disable monitoring of DLL loading.
`/savetofile: <full path to XML file>`	Export the specified rules to the indicated file in XML format.
`/savetofile: <the fullname to XML file>`	Save the list of rules to file.
`/savetofile: <the fullname to XML file> /sdc`	Save the list of Software Distribution Control rules to file.
`/clearsdc`	Delete all Software Distribution Control rules from the list.

Rule Generator for Applications Launch Control: KAVSHELL APPCONTROL /GENERATE

You can use the `KAVSHELL APPCONTROL /GENERATE` command to generate Applications Launch Control rule lists.

A password might be required to execute the command. To enter the current password, use `[/pwd:<password>]`.

KAVSHELL APPCONTROL /GENERATE command syntax

```
KAVSHELL APPCONTROL /GENERATE <path to folder> | /source:<path to file with folders list>
[/masks:<edms>] [/runapp] [/rules:<ch|cp|h>] [/strong] [/user:<user or group of users>]
[/export:<path to XML file>] [/import:<a|r|m>] [/prefix:<prefix for rules names>]
[/unique]
```

KAVSHELL APPCONTROL /GENERATE command examples

To generate rules for files from specified folders, execute the following command:

```
KAVSHELL APPCONTROL /GENERATE /source:c\folderslist.txt
/export:c:\rules\appctrlrules.xml
```

To generate rules for executable files with any extension in the specified folder and, upon the task completion, save the generated rules in the specified file XML file, execute the following command:

```
KAVSHELL APPCONTROL /GENERATE c:\folder /masks:edms /export:c\rules\appctrlrules.xml
```

You can use command-line parameters/options to configure automatic rule generation settings for the Applications Launch Control task (see the table below).

`KAVSHELL APPCONTROL /GENERATE` command-line parameters/options

Parameter/option	Description
Allowing rules usage scope	
<path to folder>	Specify the path to the folder with executable files for which allowing rules will be automatically generated.
/source: <path to file with folders list>	Specify the path to a TXT file with a list of folders with executable files for which allowing rules will be automatically generated.
/masks: <edms>	Specify the extensions of executable files for which allowing rules will be automatically generated. You can include files with the following extensions in the rules scope: • e - EXE files • d - DLL files • m - MSI files • s - scripts
/runapp	When generating allowing rules, account for applications currently running on the protected device.
Actions when automatically generating allowing rules	
/rules: <ch|cp|h>	Specify actions to perform while generating allowing rules for the Applications Launch Control task: • ch – Use the digital certificate. If the certificate is missing, use the SHA256 hash. • cp – Use the digital certificate. If the certificate is missing, use the path to the executable file.

	• h - Use the SHA256 hash.
/strong	Use the digital certificate's subject and thumbprint while automatically generating allowing rules for the Applications Launch Control task. The command is executed if a value is specified for the /rules: <ch|cp> option.
/user: <user or group of users>	Specify the user or group of users for which the rules will be applied. The application will monitor any applications run by the specified user and / or group of users.
Actions on completion of the Rule Generator for Applications Launch Control task	
/export: <full path to XML file>	Save the generated rules to an XML file.
/unique	Add information about the protected device with installed applications that are the basis for generating the Applications Launch Control allowing rules.
/prefix: <prefix for rule names>	Specify a prefix for the names of Applications Launch Control allowing rules.
/import: <a|r|m>	Import the generated rules into the specified list of Applications Launch Control rules according to the selected import rule: • a - **Add to existing rules** (rules with identical settings are duplicated) • r - **Replace existing rules** (rules with identical settings are not added; a rule is added if at least one rule setting is unique) • m - **Merge with existing rules** (rules with identical settings are not added; a rule is added if at least one rule setting is unique)

Filling the list of Applications Launch Control rules. KAVSHELL APPCONTROL

You can use the `KAVSHELL APPCONTROL` command to add rules from an XML file to the Applications Launch Control task's rule list according to the selected import rule and to delete all existing rules from the list.

A password might be required to execute the command. To enter the current password, use `[/pwd: <password>]`.

KAVSHELL APPCONTROL command syntax

```
KAVSHELL APPCONTROL /append <path to XML file> | /replace <path to XML file> | /merge
<path to XML file> | /clear
```

KAVSHELL APPCONTROL command examples

To add rules from an XML file to existing Applications Launch Control rules according to the Add to existing rules import rule, execute the following command:

```
KAVSHELL APPCONTROL /append c:\rules\appctrlrules.xml
```

You can use command-line options to select principle to add new rules from the specified XML file to the defined list of Applications Launch Control rules (see the table below).

KAVSHELL APPCONTROL command-line parameters/options

Parameter/option	Description
/append <path to XML file>	Update the list of Applications Launch Control rules based on the specified XML file. Import rule - **Add to existing rules** (rules with identical settings are duplicated).
/replace <path to XML file>	Update the list of Applications Launch Control rules based on the specified XML file. Import rule - **Replace existing rules** (rules with identical parameters are not added; the rule is added if at least one rule setting is unique).
/merge <path to XML file>	Update the list of Applications Launch Control rules based on the specified XML file. Import rule - **Merge with existing rules** (new rules do not duplicate existing rules).
/clear	Clear the list of Applications Launch Control rules.

Filling the list of Device Control rules. KAVSHELL DEVCONTROL

You can use the `KAVSHELL DEVCONTROL` command to add rules from an XML file to the Device Control task's rule list according to the selected import rule and to delete all existing rules from the list.

A password might be required to execute the command. To enter the current password, use `[/pwd: <password>]`.

KAVSHELL DEVCONTROL command syntax

```
KAVSHELL DEVCONTROL /append <path to XML file> | /replace <path to XML file> | /merge <path to XML file> | /clear
```

KAVSHELL DEVCONTROL command examples

To add rules from an XML file to the existing device control rules according to Add to existing rules import rule, execute the following command:

```
KAVSHELL DEVCONTROL /append c:\rules\devctrlrules.xml
```

You can use command-line options to select the import rule used to add new rules from the specified XML file to the defined list of Device Control rules (see the table below).

KAVSHELL DEVCONTROL command-line parameters/options

Key	Description
/append <path to XML file>	Update the list of Device Control rules based on the specified XML file. Import rule - **Add to existing rules** (rules with identical settings are duplicated).
/replace <path to XML file>	Update the list of Device Control rules based on the specified XML file. Import rule - **Replace existing rules** (rules with identical parameters are not added; the rule is added if at least one rule setting is unique).

/merge <path to XML file>	Update the list of Device Control rules based on the specified XML file. Import rule - **Merge with existing rules** (new rules do not duplicate existing rules).
/clear	Clear the list of Device Control rules.

Starting the Database Update task: KAVSHELL UPDATE

The `KAVSHELL UPDATE` command can be used to start the Kaspersky Embedded Systems Security for Windows Database Update task in synchronous mode.

A Database Update task started using the `KAVSHELL UPDATE` command is a temporary task. It is only displayed in the Application Console while being executed. However, a task log is generated and displayed in the **Task logs** in the Application Console. Kaspersky Security Center policies may apply to update tasks created and started using the `KAVSHELL UPDATE` command and update tasks created in the Application Console. For information about using Kaspersky Security Center to manage Kaspersky Embedded Systems Security for Windows on protected devices, see Section "Managing Kaspersky Embedded Systems Security for Windows using Kaspersky Security Center".

Environment variables can be used when specifying the path to an update source in this task. If a user environment variable is used, run the `KAVSHELL UPDATE` command as the corresponding user.

KAVSHELL UPDATE command syntax

```
KAVSHELL UPDATE < Path to update source | /AK | /KL> [/NOUSEKL] [/PROXY:<address>:<port>]
[/AUTHTYPE:<0-2>] [/PROXYUSER:<user name>] [/PROXYPWD:<password>] [/NOPROXYFORKL]
[/USEPROXYFORCUSTOM] [/NOFTPPASSIVE] [/REG:<iso3166 code>] [/W:<path to task log file>]
[/ALIAS:<task alias>]
```

The KAVSHELL UPDATE command has both mandatory and optional parameters/options (see the following table).

KAVSHELL UPDATE command examples

To start a custom Database Update task, execute the following command:

```
KAVSHELL UPDATE
```

To run the Database Update task using update files in the \\server\databases network folder, run the following command:

```
KAVSHELL UPDATE \\server\databases
```

To start a Database Update from the FTP server ftp://dnl-ru1.kaspersky-labs.com/ and write all task events to a file named c:\update_report.log, execute the following command:

```
KAVSHELL UPDATE ftp://dnl-ru1.kaspersky-labs.com /W:c:\update_report.log
```

To download Kaspersky Embedded Systems Security for Windows database updates from Kaspersky's update server, connect to the updates source through a proxy server (proxy server address: proxy.company.com, port: 8080). To access the protected device using the in-built Microsoft Windows NTLM authentication with user name "inetuser" and password "123456" execute the following command:

```
KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser
/PROXYPWD:123456
```

KAVSHELL UPDATE command-line parameters/options

Parameter/option	Description
Update source (mandatory parameter). Specify one or more sources. Kaspersky Embedded Systems Security for Windows will access the sources in the order in which they are listed. Separate sources with a space.	
<path in UNC format>	User-defined update source. Path to network update folder in the UNC format.
<URL>	User-defined update source. HTTP or FTP server address where the update folder is located.
<Local folder>	User-defined update source. Folder on the protected device.
/AK	Use the Kaspersky Security Center Administration server as the updates source.
/KL	Use the Kaspersky's update Servers as the update source.
/NOUSEKL	Do not use Kaspersky's update servers if other update sources are not available (used by default).
Proxy server settings	
/PROXY:<address>:<port>	Network name or IP address of the proxy server and its port. If this parameter is not specified, Kaspersky Embedded Systems Security for Windows will automatically detect the proxy server settings used in the local area network.
/AUTHTYPE:<0-2>	This parameter specifies the authentication method used to access the proxy server. It can have the following values: **0** – Microsoft Windows NTLM authentication; Kaspersky Embedded Systems Security for Windows will contact the proxy server using the **Local system** (**SYSTEM**) account **1** – Microsoft Windows NTLM authentication; Kaspersky Embedded Systems Security for Windows will contact the proxy server using the user name and password specified by the /PROXYUSER and /PROXYPWD parameters **2** – Authentication using the user name and password specified by the /PROXYUSER and /PROXYPWD parameters (basic authentication) If the proxy server does not require authentication, there is no need to specify this parameter.
/PROXYUSER:<user name>	User name that will be used to access the proxy server. If /AUTHTYPE:0 is specified, then the /PROXYUSER:<user name> and /PROXYPWD:<password> parameters will be ignored.
/PROXYPWD:<password>	User password that will be used to access the proxy server. If /AUTHTYPE:0 is specified, then the /PROXYUSER:<user name> and /PROXYPWD:<password> parameters will be ignored. If the /PROXYUSER parameter is specified and the /PROXYPWD parameter is omitted, the password will be considered an empty string.
/NOPROXYFORKL	Do not use proxy server settings to connect to Kaspersky's update servers (used by default).
/USEPROXYFORCUSTOM	Use proxy server settings to connect to user-defined update sources (not used by default).
/USEPROXYFORLOCAL	Use proxy server settings to connect to local update sources. If not specified, the **Do not use proxy server for local addresses** setting will apply.
General FTP and HTTP server settings	

/NOFTPPASSIVE	If this key is specified, Kaspersky Embedded Systems Security for Windows will use active FTP server mode to connect to the protected device. If this key is not specified, Kaspersky Embedded Systems Security for Windows will use the passive FTP server mode, if possible.
/TIMEOUT:<number of seconds>	FTP or HTTP server connection timeout. If you do not specify this parameter, Kaspersky Embedded Systems Security for Windows will use the default value of 10 seconds. The parameter value must be a whole number.
/REG:<iso3166 code>	Regional settings. This parameter is used when receiving updates from Kaspersky's update servers. Kaspersky Embedded Systems Security for Windows minimizes the load on the protected device by selecting the closest update server. The value of this parameter should be the ISO 3166-1 alpha-2 code of the country where the protected device is located, for example /REG: gr or /REG:US. If this option is omitted or an invalid country code is specified, Kaspersky Embedded Systems Security for Windows will detect the location of the protected device based on the regional settings of the protected device where the Application Console is installed.
/ALIAS:<task alias>	This parameter lets you assign a temporary name to the task, allowing you to reference the task while it runs. For example, task statistics can be viewed using the TASK command. The task alias must be unique among the task aliases of all Kaspersky Embedded Systems Security for Windows components. If this key is not specified, a temporary name in the form update_<kavshell_pid> is used; for example, update_1234. In the Application Console, the task is assigned the name "Update-databases <date time>"; for example, Update-databases 8/16/2007 5:41:02 PM.
/W:<path to task log file>	If this parameter is specified, Kaspersky Embedded Systems Security for Windows will save the task log file using the name specified by the parameter value. The log file contains task execution statistics, the time when the task was started and completed (stopped), and information about events that occurred during the task. The log is used to register events defined by the task log settings and the Kaspersky Embedded Systems Security for Windows event log settings in Event Viewer. You can specify either the absolute or relative path to the log file. If you specify only a filename without a path, the log file will be created in the current folder. Restarting the command with the same log settings will overwrite the existing log file. The log file can be viewed while a task is running. The log appears in the **Task logs** node of the Application Console. If Kaspersky Embedded Systems Security for Windows fails to create the log file, it will display an error message but will still execute the command.

Return codes for the KAVSHELL UPDATE command.

Rolling back Kaspersky Embedded Systems Security for Windows database updates: KAVSHELL ROLLBACK

The `KAVSHELL ROLLBACK` command can be used to perform a Rollback of Database Update local system task (rolls back Kaspersky Embedded Systems Security for Windows databases to the previously installed version). The command is performed synchronously.

Command syntax

```
KAVSHELL ROLLBACK
```

Return codes for the KAVSHELL ROLLBACK command.

Managing Log Inspection: KAVSHELL TASK LOG-INSPECTOR

The `KAVSHELL TASK LOG-INSPECTOR` command can be used to monitor the integrity of the environment based on an inspection of the Windows Event Log.

Command syntax

```
KAVSHELL TASK LOG-INSPECTOR
```

Command examples

```
KAVSHELL TASK LOG-INSPECTOR /stop
```

KAVSHELL TASK LOG-INSPECTOR command-line options/parameters

Parameter/option	Description
/START	Start the specified task in asynchronous mode.
/STOP	Stop the specified task.
/STATE	Return the current task status (for example, *Running*, *Completed*, *Paused*, *Stopped*, *Failed*, *Starting*, *Resuming*)
/STATISTICS	Retrieve task statistics - Information about the number of objects processed from the time the task started.

Return codes for the KAVSHELL TASK LOG-INSPECTOR command.

Activation of Application. KAVSHELL LICENSE

Kaspersky Embedded Systems Security for Windows keys and activation codes can be managed using the `KAVSHELL LICENSE` command.

A password might be required to execute the command. To enter the current password, use `[/pwd:<password>]`.

KAVSHELL LICENSE command syntax

```
KAVSHELL LICENSE [/ADD:<key file | activation code> [/R] | /DEL:<key | activation code number>]
```

KAVSHELL LICENSE command examples

To activate the application, execute the command:

```
KAVSHELL.EXE LICENSE /ADD: <activation code or key>
```

To view information on added keys, execute the command:

```
KAVSHELL LICENSE
```

To remove an added key with number 0000-000000-00000001, execute the command:

```
KAVSHELL LICENSE /DEL:0000-000000-00000001
```

The `KAVSHELL LICENSE` command can run with or without keys (see the table below).

KAVSHELL LICENSE command-line parameters/options

Setting	Description
Without keys	The command returns the following information about added keys: • Key. • License type (commercial). • Duration of the license associated with the key. • Key status (active or additional). If the status is *, the key was added as an additional key.
/ADD:<key file name or activation code>	Add a key via the specified file or an activation code. System environment variables can be used when specifying the path to a key file; user environment variables are not allowed.
/R	The /R activation code or key is in addition to the /ADD activation code or key and indicates that the activation code or key being added is an additional activation code or key.
/DEL:<key or activation code>	Deletes the key with the specified number or activation code.

Return codes for the KAVSHELL LICENSE command.

Enabling, configuring, and disabling trace logs. KAVSHELL TRACE

The `KAVSHELL TRACE` command can be used to enable and disable the trace log for all Kaspersky Embedded Systems Security for Windows subsystems and to set the log detail level.

Kaspersky Embedded Systems Security for Windows writes information to trace files and the dump file in unencrypted form.

KAVSHELL TRACE command syntax

```
KAVSHELL TRACE </ON /F:<path to folder with trace files> [/S:<maximum size of the log file in megabytes>] [/LVL: debug|info|warning|error|critical] [/r: <maximum number of trace files to rotate>] | /OFF>
```

If the trace log is enabled and you wish to change its settings, enter the `KAVSHELL TRACE` command with the /ON option and use the /S and /LVL parameters to specify the trace log settings (see the table below).

KAVSHELL TRACE command keys

Key	Description
`/ON`	Enables the trace log.
`/F:<folder with trace files>`	This parameter specifies the full path to the folder where trace log files will be saved (required). If a path to a non-existent folder is specified, no trace log will be created. Paths to folders on the network drives of other protected devices cannot be specified. If the path specified by the parameter has a space, it needs to be enclosed in quotes, for example, /F:"C:\Trace Folder". System environment variables can be used when specifying the path to the trace log files; user environment variables are not allowed.
`/S: <maximum log file size in megabytes>`	This key sets the maximum size of a single trace log file. As soon as the log file reaches the maximum size, Kaspersky Embedded Systems Security for Windows will start recording information in a new file; the previous log file will be saved. If the value of this parameter is not specified, the maximum size of one log file will be 50 MB.
`/LVL:debug|info|warning|error|critical`	This parameter sets the log detail level from maximum (**All debug information**), in which all events are recorded in the log, to minimum (**Critical events**), in which only critical events are recorded. If this parameter is not specified, all events included in the **All debug information** level of detail will be recorded in the trace log.
`/r:<maximum number of trace files to rotate>`	This option enables rotation of trace files. If trace log rotation is enabled and the maximum number of log files for rotation is reached, the oldest file is deleted before a new file is created. Available values: from 1 to 999. If no value is specified, trace file rotation is not enabled and the application returns an error.
/OFF	This option disables the trace log.

KAVSHELL TRACE command example

*To enable the trace log using the **All debug information** level of detail and a maximum log size of 200MB, saving the log file to the "C:\Trace Folder" folder, execute the command:*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /S:200
```

*To enable the trace log using the **Important events** level of detail, saving the log file to the "C:\Trace Folder" folder, execute the command:*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning
```

*To enable the trace log using the **Important events** level of detail, save the log file to C:\Trace Folder, and enable trace file rotation upon reaching a maximum of 50 files, execute the following command:*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning /r:50
```

To disable the trace log, execute the command:

```
KAVSHELL TRACE /OFF
```

Return codes for the KAVSHELL TRACE command.

Kaspersky Embedded Systems Security for Windows log files defragmentation. KAVSHELL VACUUM

You can use the `KAVSHELL VACUUM` command to defragment the application's log files. This helps avoid system and application errors due to storing a large number of log files containing application events.

A password might be required to execute the command. To enter the current password, use `[/pwd:<password>]`.

We recommend that you apply the `KAVSHELL VACUUM` command to optimize log file storage in case On-Demand Scan and update tasks are run frequently. This command causes Kaspersky Embedded Systems Security for Windows update the logical structure of the application's log files stored on a protected device at the specified path.

By default, the application's log files are stored at "C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\3.4\Reports". If you have manually specified another path for storing logs, the `KAVSHELL VACUUM` command defragments the files in the folder specified in the Kaspersky Embedded Systems Security for Windows log settings.

Large file sizes increase the time required for the `KAVSHELL VACUUM` command to complete the defragment operation.

The Real-Time Protection and Computer Control tasks are not available while the `KAVSHELL VACUUM` command is executed. The defragmentation process blocks access to the Kaspersky Embedded Systems Security for Windows log and prevents event logging. To avoid a reduction in protection, we recommend that you plan when you will run the `KAVSHELL VACUUM` command.

To defragment the Kaspersky Embedded Systems Security for Windows log files, execute the following command:

```
KAVSHELL VACUUM
```

This command requires Local System account rights.

Cleaning iSwift base. KAVSHELL FBRESET

Kaspersky Embedded Systems Security for Windows uses iSwift technology, which lets the application avoid rescanning files that have not been modified since the last scan (**Use iSwift technology**).

Kaspersky Embedded Systems Security for Windows creates klamfb.dat and klamfb2.dat files in the "%SYSTEMDRIVE%\System Volume Information" folder. These files contain information about clean objects that have already been scanned. The klamfb.dat (klamfb2.dat) file grows with the number of files scanned by Kaspersky Embedded Systems Security for Windows. It only contains current information about files in the system: if a file is removed, Kaspersky Embedded Systems Security for Windows purges the corresponding information from klamfb.dat.

To clear a file, use the `KAVSHELL FBRESET` command.

Please keep in mind the following specifics when using the `KAVSHELL FBRESET` command:

- When using the KAVSHELL FBRESET command to clear the klamfb.dat file, Kaspersky Embedded Systems Security for Windows does not pause the protection (unlike what happens if klamfb.dat is deleted manually).
- Kaspersky Embedded Systems Security for Windows may increase the protected device workload after the data in klamfb.dat is cleared. In this case, Kaspersky Embedded Systems Security for Windows scans all files accessed for the first time after klamfb.dat is cleared. After the scan, Kaspersky Embedded Systems Security for Windows puts information about each scanned object back into klamfb.dat. If there are new attempts to access an object, iSwift technology prevents rescanning of the file if it has not been changed.

The `KAVSHELL FBRESET` command is available only if the command-line interpreter is started under the SYSTEM account.

Enabling and disabling dump file creation. KAVSHELL DUMP

You can use the `KAVSHELL DUMP` command to enable or disable creation of snapshots (dump files) of Kaspersky Embedded Systems Security for Windows processes if they terminate abnormally (see the following table). Additionally, you can create a dump file of running Kaspersky Embedded Systems Security for Windows processes at any time.

To create a dump file successfully, the `KAVSHELL DUMP` command must be executed under the local system account (SYSTEM).

Kaspersky Embedded Systems Security for Windows writes information to trace files and the dump file in unencrypted form.

The KAVSHELL DUMP command can not be used for x64 processes.

KAVSHELL DUMP command syntax

```
KAVSHELL DUMP </ON /F:<folder with the dump file>|/SNAPSHOT /F:< folder with the dump file> /P:<pid> | /OFF>
```

KAVSHELL DUMP command-line parameters/options

Key	Description
/ON	Enables creation of a dump file if a process terminates abnormally.
/F:<path to folder with dump files>	This is a mandatory parameter. It specifies the path to the folder where the dump file will be saved. Paths to folders on the network drives of other unprotected devices are not allowed. System environment variables can be used when specifying the path to the folder for the dump file; user environment variables are not allowed.
/SNAPSHOT	Takes a snapshot of the memory of the running process with the specified PID and saves the dump file in the folder specified by the /F parameter.
/P	The process identifier (PID) is displayed in the Microsoft Windows Task Manager.
/OFF	Disables the creation of a dump file if a process terminates abnormally.

Return codes for the KAVSHELL DUMP command.

KAVSHELL DUMP command example

To enable creation of a dump file; saving the dump file to the "C:\Dump Folder" folder, execute the command:

```
KAVSHELL DUMP /ON /F:"C:\Dump Folder"
```

To make a dump for the process with ID 1234 in the "C:/Dumps" folder, execute the command:

```
KAVSHELL DUMP /SNAPSHOT /F:C:\dumps /P:1234
```

To disable creation of dump files, execute the command:

```
KAVSHELL DUMP /OFF
```

Importing settings. KAVSHELL IMPORT

The `KAVSHELL IMPORT` command lets you import the settings of Kaspersky Embedded Systems Security for Windows and its current tasks from a configuration file to a copy of Kaspersky Embedded Systems Security for Windows on the protected device. A configuration file can be created using the `KAVSHELL EXPORT` command.

A password might be required to execute the command. To enter the current password, use `[/pwd:<password>]`.

KAVSHELL IMPORT command syntax

```
KAVSHELL IMPORT <name of configuration file and path to file>
```

KAVSHELL IMPORT command examples

```
KAVSHELL IMPORT Host1.xml
```

KAVSHELL IMPORT command-line parameter

Setting	Description
<name of configuration file and path to file>	Name of configuration file used as the import source for settings. System environment variables can be used when specifying the path to the file; user environment variables are not allowed.

Return codes for the KAVSHELL IMPORT command.

Exporting settings. KAVSHELL EXPORT

The `KAVSHELL EXPORT` command lets you export all of the settings of Kaspersky Embedded Systems Security for Windows and its current tasks to a configuration file in order to import them later into copies of Kaspersky Embedded Systems Security for Windows installed on another protected device.

KAVSHELL EXPORT command syntax

```
KAVSHELL EXPORT <name of configuration file and path to file>
```

KAVSHELL EXPORT command examples

```
KAVSHELL EXPORT Host1.xml
```

KAVSHELL EXPORT command-line parameters

Setting	Description
<name of configuration file and path to file>	Name of the configuration file that will contain the settings. Any file extension can be assigned to the configuration file. System environment variables can be used when specifying the path to the file; user environment variables are not allowed.

Return codes for the KAVSHELL EXPORT command.

Integration with Microsoft Operations Management Suite. KAVSHELL OMSINFO

The KAVSHELL OMSINFO command lets you review the status of the application and information about threats detected by anti-virus databases. The information about threats is taken from the available event logs.

KAVSHELL OMSINFO command syntax

```
KAVSHELL OMSINFO <full path to generated file with file name>
```

KAVSHELL OMSINFO command examples

```
KAVSHELL OMSINFO C:\Users\Admin\Desktop\omsinfo.json
```

KAVSHELL OMSINFO command-line parameter

Setting	Description
<path to generated file with file name>	Name of the generated file that will contain information about the application status and any detected threats.

Managing the Baseline File Integrity Monitor task: KAVSHELL FIM /BASELINE

You can use the `KAVSHELL FIM /BASELINE` command to configure the mode in which the Baseline File Integrity Monitor task runs and monitors the loading of DLL modules.

A password might be required to execute the command. To enter the current password, use `[/pwd:<password>]`.

KAVSHELL FIM /BASELINE command syntax

```
KAVSHELL FIM /BASELINE [/CREATE: [<monitoring scope> | /L:<path to TXT file containing the list of monitoring scopes>] [/MD5 | /SHA256] [/SF]] | [/CLEAR [/BL:<baseline id> | /ALIAS:<existing alias>]] | [/EXPORT:<path to TXT file> [/BL:<baseline id> | /ALIAS:<existing alias>]] | [/SHOW [/BL:<baseline id> | /ALIAS:<existing alias>]] | [/SCAN [/BL:<baseline id> | /ALIAS:<existing alias>]] | [/PWD:<password>]
```

KAVSHELL FIM /BASELINE command examples

To delete a baseline, run the following command:

```
KAVSHELL FIM /BASELINE /CLEAR /BL:<baseline id>
```

You can configure Baseline File Integrity Monitor task settings using the command-line options (see the table below).

`KAVSHELL FIM /BASELINE` command-line parameters/options

Parameter/option	Description
`/CREATE`	Create a new Baseline File Integrity Monitor task. Kaspersky Embedded Systems Security for Windows will start the new Baseline File Integrity Monitor task in order to create a baseline.
`/L`	Specify the path to the TXT file containing the list of monitoring scopes.
`/MD5`	Specify the MD5 algorithm for calculating a checksum (optional parameter). `/MD5` parameter can not be used together with `/SHA256`.

	MD5 algorithm is used by default.
/SHA256	Specify the SHA256 algorithm for calculating a checksum (optional parameter). /SHA256 parameter can not be used together with /MD5. MD5 algorithm is used by default.
/SF	Includes all subfolders in the Baseline File Integrity Monitor task scope (optional parameter). By default all subfolders are excluded from the Baseline File Integrity Monitor task scope.
/CLEAR	Delete the baseline with specified <baseline id> or the baseline for the task with specified <existing alias>. Delete all baselines if neither <baseline id> nor <existing alias> was specified. Optional parameter.
/BL	Specify the unique ID of a baseline (optional parameter).
/EXPORT	Export the data about all baselines in a TXT file.
/SHOW	Show data about all baselines.
/SCAN	Start the new Baseline File Integrity Monitor task with specified <baseline id> or specified <existing alias>.
/ALIAS	Specify the name of an existing task or the name for a new task.
<monitoring scope>	Specify the file or folder that you want to include in the Baseline File Integrity Monitor task scope. This parameter allows to specify only one area.
<path to TXT file containing the list of monitoring scopes>	Specify the path to the TXT file containing the list of monitoring scopes. The file must be UTF-8 encoded, and each path to a monitoring scope must be specified in a separate row.
<path to TXT file>	Specify the path to the file to which you want to export the data about all baselines.
<baseline id>	Specify the unique ID of a baseline. You can use the /SHOW parameter to learn the ID of a baseline.
<existing alias>	Specify the name of an existing task.
<new alias>	Specify the name of a new task.

Command return codes

Return code for the KAVSHELL START and KAVSHELL STOP commands

Return code for the KAVSHELL START and KAVSHELL STOP commands

Return	Description

code	
0	Operation completed successfully
-3	Permission error
-5	Invalid command syntax
-6	Invalid operation (for example, the Kaspersky Security Service is already running or already stopped)
-7	Service not registered
-8	Automatic Service startup is disabled.
-9	Attempt to start the protected device under another user account failed (by default, the Kaspersky Security Service runs under the Local system user account)
-99	Unknown error

Return code for KAVSHELL SCAN and KAVSHELL SCANCRITICAL commands

Return code for KAVSHELL SCAN and KAVSHELL SCANCRITICAL commands

Return code	Description
0	Operation completed successfully (no threats detected)
1	Operation canceled
-2	Service not running
-3	Permission error
-4	Object not found (file with the list of scan scopes not found)
-5	Invalid command syntax or scan scope not defined
-80	Infected and other objects detected
-81	Probably infected objects detected
-82	Processing errors detected
-83	Unscanned objects found
-84	Corrupted objects detected
-85	Failed to create task log
-99	Unknown error
-301	Invalid key

Return code for the KAVSHELL TASK LOG-INSPECTOR command

Return code for the KAVSHELL TASK LOG-INSPECTOR command

Return code	Description
0	Operation completed successfully

-6	Invalid operation (for example, the Kaspersky Security Service is already running or already stopped)
402	Task is already running (for the /STATE option)

Return codes for the KAVSHELL TASK command

Return codes for the KAVSHELL TASK command

Return code	Description
0	Operation completed successfully
-2	Service not running
-3	Permission error
-4	Object not found (task not found)
-5	Invalid command syntax
-6	Invalid operation (for example, task not running, already running, or cannot be paused)
-99	Unknown error
-301	Invalid key
401	Task not running (for the /STATE option)
402	Task is already running (for the /STATE option)
403	Task already paused (for the /STATE option)
-404	Operation failed (a change in task status resulted in a crash)

Return codes for the KAVSHELL RTP command

Return codes for the KAVSHELL RTP command

Return code	Description
0	Operation completed successfully
-2	Service not running
-3	Permission error
-4	Object not found (one or all of the Real-Time Computer Protection tasks not found)
-5	Invalid command syntax
-6	Invalid operation (for example, the task is already running or already stopped)
-99	Unknown error
-301	Invalid key

Return codes for the KAVSHELL UPDATE command

Return codes for the KAVSHELL UPDATE command

Return code	Description
0	Operation completed successfully
200	All objects are up-to-date (database or program components are current)
-2	Service not running
-3	Permission error
-5	Invalid command syntax
-99	Unknown error
-206	Extension files are missing in the specified source or have unknown format
-209	Error while connecting to the update source
-232	Authentication error while connecting to proxy server
-234	Error while connecting to Kaspersky Security Center
-235	Kaspersky Embedded Systems Security for Windows was not authenticated when connecting to the update source
-236	Application database is corrupted
-301	Invalid key

Return codes for the KAVSHELL ROLLBACK command

Return codes for the KAVSHELL ROLLBACK command

Return code	Description
0	Operation completed successfully
-2	Service not running
-3	Permission error
-99	Unknown error
-221	Backup copy of database not found or corrupted
-222	Backup copy of database corrupted

Return codes for the KAVSHELL LICENSE command

Return codes for the KAVSHELL LICENSE command

Return code	Description
0	Operation completed successfully
-2	Service not running
-3	Insufficient privileges to manage keys
-4	Key with specified number not found
-5	Invalid command syntax

-6	Invalid operation (key already added)
-99	Unknown error
-301	Invalid key
-303	License applies to a different application

Return codes for the KAVSHELL TRACE command

Return codes for the KAVSHELL TRACE command

Return code	Description
0	Operation completed successfully
-2	Service not running
-3	Permission error
-4	Object not found (path specified for the trace log folder not found)
-5	Invalid command syntax
-6	Invalid operation (attempt to execute the KAVSHELL TRACE /OFF command when trace logs are already disabled)
-99	Unknown error

Return codes for the KAVSHELL FBRESET command

Return codes for the KAVSHELL FBRESET command

Return code	Description
0	Operation completed successfully
-99	Unknown error

Return codes for the KAVSHELL DUMP command

Return codes for the KAVSHELL DUMP command

Return code	Description
0	Operation completed successfully
-2	Service not running
-3	Permission error
-4	Object not found (path specified for dump file folder not found; process with specified PID not found)
-5	Invalid command syntax
-6	Invalid operation (attempt of KAVSHELL DUMP/OFF command execution if dump file creation is already disabled)

-99	Unknown error

Return codes for the KAVSHELL IMPORT command

Return codes for the KAVSHELL IMPORT command

Return code	Description
0	Operation completed successfully
-2	Service not running
-3	Permission error
-4	Object not found (unable to find a configuration file that can be imported)
-5	Invalid syntax
-99	Unknown error
501	Operation completed successfully with an error/comment, for example, Kaspersky Embedded Systems Security for Windows did not import parameters for some functional component
-502	Import file is missing or has an unrecognized format
-503	Incompatible settings (configuration file exported from a different program or a later and incompatible version of Kaspersky Embedded Systems Security for Windows)

Return codes for the KAVSHELL EXPORT command

Return codes for the KAVSHELL EXPORT command

Return code	Description
0	Operation completed successfully
-2	Service not running
-3	Permission error
-5	Invalid syntax
-10	Unable to create a configuration file (for example no access to the folder specified in the path to the file)
-99	Unknown error
501	Operation completed successfully with an error/comment, for example, Kaspersky Embedded Systems Security for Windows did not export parameters for some functional component

Return codes for the KAVSHELL FIM /BASELINE command

Return codes for the KAVSHELL FIM /BASELINE command

Return code	Description

0	Operation completed successfully
-2	Service not running
-3	Permission error
-4	Object not found (task not found)
-5	Invalid command syntax
-6	Invalid operation (for example, the baseline already was deleted)
-10	Unable to create a configuration file (for example no access to the folder specified in the path to the file)
-12	Invalid password
-80	Inconsistent with the baseline objects detected
-85	Failed to create task log
-99	Internal error
-303	Invalid license key
-502	Task not running
200	All objects are consistent with the baseline
501	Task completed successfully with an error/comment

Contacting Technical Support

This section describes the ways to receive technical support and the conditions on which it is available.

How to get technical support

If you cannot find a solution to your problem in the application documentation or in one of the sources of information about the application, we recommend that you contact Technical Support. Technical Support specialists will answer your questions about installing and using the application.

Technical support is available only to users who have purchased a commercial license for the application. Technical support is not available to users who have a trial license.

Application support is provided according to the application lifecycle (see the application lifecycle page).

Before contacting Technical Support, please read through the Technical Support rules.

You can contact Technical Support by sending a request to Kaspersky Technical Support through the Kaspersky CompanyAccount portal.

Technical Support via Kaspersky CompanyAccount

Kaspersky CompanyAccount is a portal for companies that use Kaspersky applications. Kaspersky CompanyAccount is designed to facilitate interaction between users and Kaspersky specialists via online requests. Kaspersky CompanyAccount lets you monitor the progress of electronic request processing by Kaspersky specialists and store a history of electronic requests.

You can register all of your organization's employees under a single user account on Kaspersky CompanyAccount. A single account lets you centrally manage electronic requests from registered employees to Kaspersky and also manage the privileges of these employees via Kaspersky CompanyAccount.

Kaspersky CompanyAccount is available in the following languages:

- English
- Spanish
- Italian
- German
- Polish
- Portuguese
- Russian
- French

- Japanese

To learn more about Kaspersky CompanyAccount, visit the Technical Support website.

Using trace files and AVZ scripts

After you report a problem to Kaspersky Technical Support specialists, they may ask you to generate a report with information about the operation of Kaspersky Embedded Systems Security for Windows and to send it to Kaspersky Technical Support. Kaspersky Technical Support specialists may also ask you to create a trace file. The trace file allows following the process of how application commands are performed, step by step, in order to determine the stage of application operation at which an error occurs.

After analyzing the data you send, Kaspersky Technical Support specialists can create an AVZ script and send it to you. With AVZ scripts, it is possible to analyze active processes for threats, scan the protected device for threats, disinfect or delete infected files, and create system scan reports.

Glossary

Active key

A key that is currently being used by the application.

Administration Server

A component of Kaspersky Security Center that centrally stores information about Kaspersky applications installed on the corporate network, and manages them.

Anti-virus databases

Databases that contain information about computer security threats known to Kaspersky as of when the anti-virus databases are released. Anti-virus database entries make it possible to detect malicious code in scanned objects. Anti-virus databases are created by Kaspersky experts and updated hourly.

Archive

One or more file(s) packaged into a single file through compression. A dedicated application, called an archiver, is required for packing and unpacking the data.

Backup

Special storage intended for saving backup copies of objects before they are disinfected or deleted.

Disinfection

A method of processing infected objects that results in full or partial recovery of data. Not all infected objects can be disinfected.

Event importance

Property of an event encountered during the operation of a Kaspersky application. There are four importance levels:

- Critical event.
- Functional failure.
- Warning.

- Info.

Events of the same type can have different importance levels depending on the situation in which the event occurred.

False positive

A situation where a Kaspersky application considers a non-infected object to be infected because the object's code is similar to that of a virus.

File mask

A representation of a file name using generic characters. The main characters used in file masks are * and ? (where * stands for any number of any characters, and ? stands for any single character).

Heuristic analyzer

A technology for detecting threats about which information has not yet been added to Kaspersky databases. The heuristic analyzer detects objects whose behavior in the operating system may pose a security threat. Objects detected by the heuristic analyzer are considered to be probably infected. For example, an object may be considered probably infected if it contains sequences of commands that are typical of malicious objects (open file, write to file).

Infectable file

A file that, due to its structure or format, can be used by criminals as a "container" to store and spread malicious code. As a rule, these are executable files with such file extensions as .com, .exe, .dll, and others. The risk that malicious code will intrude into such files is quite high.

Infected object

An object in which a section of code completely matches a section of code of a known threat. Kaspersky experts do not recommend that you work with such objects.

Kaspersky Security Network (KSN)

Cloud services infrastructure that provides access to Kaspersky's online knowledge base about the reputation of files, web resources, and software. Using data from Kaspersky Security Network ensures faster responses by Kaspersky applications to threats, improves the performance of some protection components, and reduces the likelihood of false positives.

License term

The period of time during which you can use the application functions and additional services. The scope of available features and additional services depends on the license type.

Local task

A task that is defined and runs on an individual client computer.

OLE object

An object attached to another file or embedded into another file through the use of the Object Linking and Embedding (OLE) technology. An example of an OLE object is a Microsoft Office Excel® spreadsheet embedded into a Microsoft Office Word document.

Policy

A policy defines application settings and manages the ability to configure that application on computers within an administration group. An individual policy must be created for each application. You can create multiple policies for applications installed on computers in each administration group, but only one policy can be applied at a time to each application within an administration group.

Protection state

The current protection status, which characterizes the security level of the device.

Quarantine

The folder to which the Kaspersky application moves probably infected objects that have been detected. Objects are stored in Quarantine in encrypted form in order to avoid any impact on the computer.

Security level

A security level is a predefined set of component settings.

SIEM

An abbreviation of Security Information and Event Management. A solution for managing information and events in the security system of an organization.

Startup objects

A set of applications needed for the operating system and software that is installed on the computer to start and operate correctly. These objects are executed every time the operating system is started. There are viruses capable of infecting such objects specifically, which may lead, for example, to blocking of operating system startup.

Task

Functions performed by the Kaspersky application are implemented as tasks, such as: Real-Time File Protection, Full Device Scan, and Database Update.

Task settings

Application settings specific to each type of task.

Update

The process of replacing or adding new files (databases or application modules) retrieved from Kaspersky update servers.

Vulnerability

A flaw in an operating system or an application that may be exploited by malware makers to penetrate the operating system or application, and corrupt its integrity. The presence of a large number of vulnerabilities in an operating system makes it unreliable, because viruses that penetrate the operating system may disrupt both the operating system and installed applications.

Information about third-party code

Information about third-party code is contained in the file legal_notices.txt, in the application installation folder.

Trademark notices

Registered trademarks and service marks are the property of their respective owners.

The Bluetooth word, mark and logos are owned by Bluetooth SIG, Inc.

Domino and Lotus Notes are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide.

Pentium is a trademark of Intel Corporation in the U.S. and/or other countries.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft, Active Directory, Excel, Forefront, Hyper-V, Internet Explorer, JScript, Lync, Outlook, PowerShell, SharePoint, SQL Server, Windows, Windows Server, Windows Vista, and Windows XP are trademarks of the Microsoft group of companies.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Limited.